CYBERPWN
EMPOWERING CYBER RESILIENCE

Static Code Analysis Report

v1.0

Prepared for: Sutherland Global Services Pvt Ltd.

6th **July** 2026

Disclaimer

This data shall not be disclosed and shall not be duplicated, used, or disclosed in whole or in part for any purpose. If a contract is awarded to 5Sec CyberPWN Technologies Pvt Ltd., as a result of or in connection with the submission of this data, the client or prospective client shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the client's or prospective client's right to use the information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is contained in all marked sheets.

CYBERPWN
EMPOWERING CYBER RESILIENCE

CONTENTS

DOCUMENT DETAILS **6**

INTRODUCTION **7**

SCOPE & DURATION 7

Type of Assessment **7**

Approach and Methodology **8**

Standards and Framework Followed **8**

Severity Rating 8

Risk Rating Definitions 9

RESULT OVERVIEW **10**

RESULT OVERVIEW SOURCE COMPOSITION ANALYSIS **13**

VULNERABILITIES DETAILS **16**

1. COMMAND INJECTION 16
2. CREDENTIAL MANAGEMENT: HARDCODED API CREDENTIALS 20
3. CROSS-SITE SCRIPTING: DOM 22
4. INSECURE SSL: SERVER IDENTITY VERIFICATION DISABLED 24
5. INSECURE TRANSPORT: MAIL TRANSMISSION 25
6. INSECURE TRANSPORT: WEAK SSL PROTOCOL 26
7. PATH MANIPULATION 27
8. PRIVACY VIOLATION 38
9. WEAK ENCRYPTION 39
10. ASP.NET MVC BAD PRACTICES: MODEL WITH REQUIRED NON-NULLABLE PROPERTY 40
11. CROSS-SITE SCRIPTING: REFLECTED 41
12. DYNAMIC CODE EVALUATION: CODE INJECTION 42
13. INSECURE RANDOMNESS 43
14. KEY MANAGEMENT: HARDCODED PBE PASSWORD 45
15. PASSWORD MANAGEMENT: EMPTY PASSWORD 46
16. PASSWORD MANAGEMENT: HARDCODED PASSWORD 47
17. PRIVACY VIOLATION: HEAP INSPECTION 49
18. PROCESS CONTROL 52
19. SERVER-SIDE REQUEST FORGERY 53
20. WEAK ENCRYPTION: INSECURE MODE OF OPERATION 55
21. XML INJECTION 57
22. XPATH INJECTION 58
23. PATH MANIPULATION: BASE PATH OVERWRITING 59
24. PATH MANIPULATION: ZIP ENTRY OVERWRITE 61
25. SYSTEM INFORMATION LEAK: EXTERNAL 62
26. WCF MISCONFIGURATION: ANONYMOUS TRANSPORT CLIENT 63
27. WCF MISCONFIGURATION: INSUFFICIENT LOGGING 65
28. WCF MISCONFIGURATION: SERVICE ENUMERATION 66
29. WCF MISCONFIGURATION: WEAK TOKEN 67
30. DENIAL OF SERVICE 69

31. DENIAL OF SERVICE: REGULAR EXPRESSION 72
32. HEADER MANIPULATION 73
33. MISSING XML VALIDATION 74
34. OFTEN MISUSED: AUTHENTICATION 75
35. PASSWORD MANAGEMENT: LACK OF KEY DERIVATION FUNCTION 76
36. PASSWORD MANAGEMENT:NULL PASSWORD 77
37. PASSWORD MANAGEMENT: PASSWORD IN COMMENT 79
38. POOR LOGGING PRACTICE: USE OF A SYSTEM OUTPUT STREAM 80
39. RESOURCE INJECTION 83
40. SETTING MANIPULATION 84
41. SYSTEM INFORMATION LEAK 85
42. SYSTEM INFORMATION LEAK: INTERNAL 89
43. UNCHECKED RETURN VALUE 92
44. UNSAFE NATIVE INVOKE 93
45. UNSAFE REFLECTION 94
46. WCF MISCONFIGURATION: THROTTLING NOT ENABLED 95
47. WEAK CRYPTOGRAPHIC HASH 96
48. WEAK CRYPTOGRAPHIC HASH: INSECURE PBE ITERATION COUNT 97
49. WEAK CRYPTOGRAPHIC HASH: USER-CONTROLLED PBE SALT 99
50. WEAK XML SCHEMA: TYPE ANY 100
51. WEAK XML SCHEMA: UNBOUNDED OCCURRENCES 102

SOURCE COMPOSITION ANALYSIS 104

1. HEAP-BASED BUFFER OVERFLOW 104
2. INTEGER OVERFLOW OR WRAPAROUND 105
3. OUT-OF-BOUNDS WRITE 106
4. USE OF EXTERNALLY-CONTROLLED FORMAT STRING 107
5. RELEASE OF INVALID POINTER OR REFERENCE 108
6. NULL POINTER DEREFERENCE 109
7. STACK-BASED BUFFER OVERFLOW 110
8. OFF-BY-ONE ERROR 111
9. ALLOCATION OF RESOURCES WITHOUT LIMITS OR THROTTLING 112
10. DIRECTORY TRAVERSAL 113
11. TIME-OF-CHECK TIME-OF-USE (TOCTOU) RACE CONDITION 114
12. ACCESS OF UNINITIALIZED POINTER 115
13. UNCONTROLLED RECURSION 116
14. USE AFTER FREE 117
15. DENIAL OF SERVICE (DOS) 118
16. INFINITE LOOP 119
17. XML EXTERNAL ENTITY (XXE) INJECTION 122
18. INSECURE DEFAULTS 125
19. IMPROPER CERTIFICATE VALIDATION 127
20. PRIVILEGE ESCALATION 128
21. INFORMATION EXPOSURE 129
22. OUT-OF-BOUNDS READ 130
23. AUTHENTICATION BYPASS 131
24. CRLF INJECTION 132

25. RESOURCE INJECTION 133
26. INSERTION OF SENSITIVE INFORMATION INTO LOG FILE 134
27. RELIANCE ON UNDEFINED, UNSPECIFIED, OR IMPLEMENTATION-DEFINED BEHAVIOR 135
28. ARBITRARY CODE INJECTION 136
29. MISSING RELEASE OF RESOURCE AFTER EFFECTIVE LIFETIME 137
30. INCOMPLETE LIST OF DISALLOWED INPUTS 138
31. UNCHECKED INPUT FOR LOOP CONDITION 139
32. MISSING RELEASE OF MEMORY AFTER EFFECTIVE LIFETIME 140
33. EXPIRED POINTER DEREFERENCE 141
34. INTEGER UNDERFLOW (WRAP OR WRAPAROUND) 142
35. IMPROPER VALIDATION OF ARRAY INDEX 143
36. INSECURE RANDOMNESS 144
37. UNSYNCHRONIZED ACCESS TO SHARED DATA IN A MULTITHREADED CONTEXT 145
38. IMPROPER AUTHENTICATION 146
39. INCORRECT CALCULATION OF BUFFER SIZE 147
40. BUFFER ACCESS WITH INCORRECT LENGTH VALUE 148
41. DIVISION BY ZERO 149
42. BUFFER OVER-READ 150
43. IMPROPER ENCODING OR ESCAPING OF OUTPUT 151

Annexure A – Source Code Review Methodology & Standards 152

Annexure B – TOOLS USED 154

Annexure C – OWASP – Source Code Review 155

DOCUMENT DETAILS

DOCUMENT CONTROL	
Document Title	**Sutherland Global Services Pvt Ltd**
Document Classification	**Final Report**
Last Edit Date	**06-July-2026**

DOCUMENT HISTORY			
DATE	**VERSION**	**PREPARED BY**	**STATUS**
06-07-2026	**1.0**	**Arham Jain**	**Final Report**

CUSTOMER INFORMATION	
Company Name	Sutherland Global Services Pvt Ltd.
Address	Gateway Office Parks Pvt. Ltd 2nd, 3rd, 4th ,5th Floor, Block B2 No:16, GST Road, Perungalathur Chennai - Tamil Nadu – 600063 – India.
Website	https://www.sutherlandglobal.com/
Contact Name	Sarfraz Amin
Title	Senior Associate Vice President

CONSULTANT INFORMATION		
Name	**Role**	**Responsibility**
Arham Jain	Lead Security Engineer	Document Preparation
Prabhu G	Lead Security Engineer	Document Review
Anuranjan Garnaik	Senior Manager	Document Approval
Sarfraz Amin	Senior Associate Vice President	Document Acceptance

INTRODUCTION

Sutherland Global Services Pvt Ltd engaged CyberPWN Technologies to carry out an assessment as included in the scope of the work. The purpose of the test was to determine security vulnerabilities of their **Source Code**. The tests were carried out assuming the identity of an attacker or a user with malicious intent. Due care was taken not to harm the provided code.

This report contains the results of Static Application Security Testing activity that was performed during the period **22 June 2026 to 06 July 2026**

SCOPE & DURATION

The scope includes Static Application Security Assessment for below mentioned application.

Application Name	Number File Scanned (Excluding Dependency)
Robility (Thick Client) – RobilityActivities, RobilityDesigner & Runner	8850

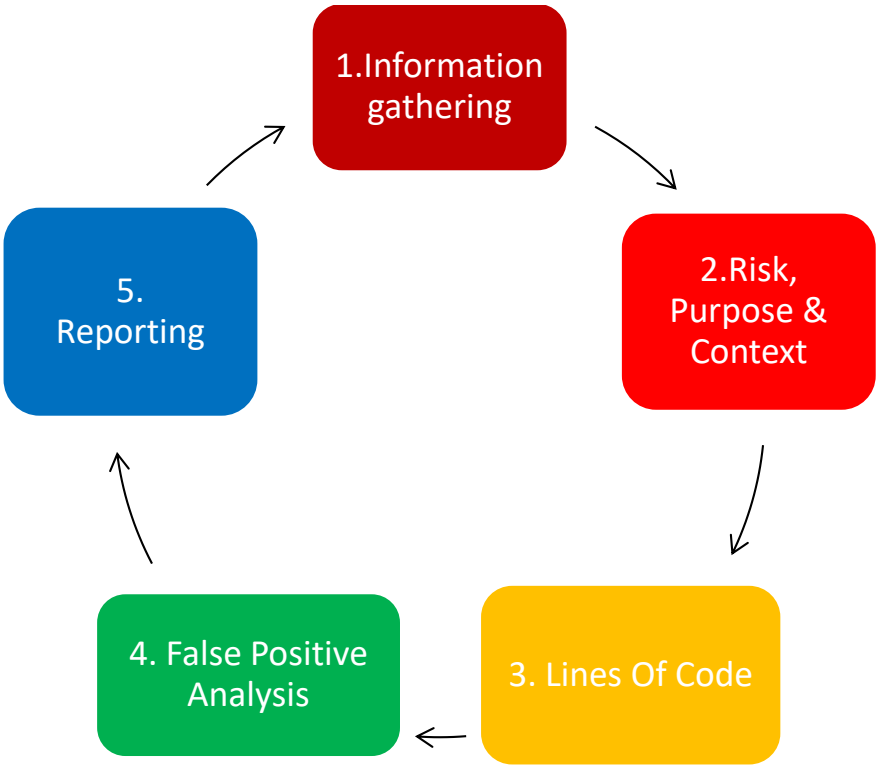
The test was performed from **22-06-2026** till **06-07-2026** including reporting.

Type of Assessment

For this engagement, the assessment was limited to the following categories:

1. Static Application Security Assessment

Approach and Methodology



For detailed definitions and details, please refer to Annexure A in this report.

Standards and Framework Followed

Our testing methodology adapts techniques and follows methodology from the OWASP source code review guide.

Severity Rating

Based on the severity of the vulnerability, they are assigned below ratings:

CVSS Severity Rating	CVSS Score
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
Informational	0.0

Risk Rating Definitions

Severity Rating	Definitions
Critical	Critical severity vulnerabilities usually have most of the following traits: • A successful attack may lead to complete compromise of the system • Exploitation can be done remotely over an untrusted connection – such as the Internet • Exploiting the vulnerability is very easy or straightforward. It may not require privilege accounts or user interaction. • It has a very significant impact on confidentiality, integrity and/or availability of the targeted system
High	High severity vulnerabilities demonstrate some of the following characteristics: • It is not straight-forward to exploit and may require some user interaction and has minimum dependency. • Usually gives an attacker elevated privilege. • It has a significant impact on confidentiality, integrity and availability
Medium	• Vulnerabilities scored medium generally: • Require specific user privileges or conditions to execute the attack. • Grant attacker access to non-critical privileged functionality/data. • Moderately affects Confidentiality, Integrity or integrity.
Low	Vulnerabilities scored low usually exhibit some of the following characteristics: • They have little impact on the confidentiality, integrity or availability of the organization's data or assets. • Requires a great amount of computational power to exploit the vulnerability. • Require excessive privileges or access to execute an attack • Exploits are not known publicly

CYBERPWN
EMPOWERING CYBER RESILIENCE

RESULT OVERVIEW

The following table summarizes the list of findings discovered during the **security assessment** and their identified risk:

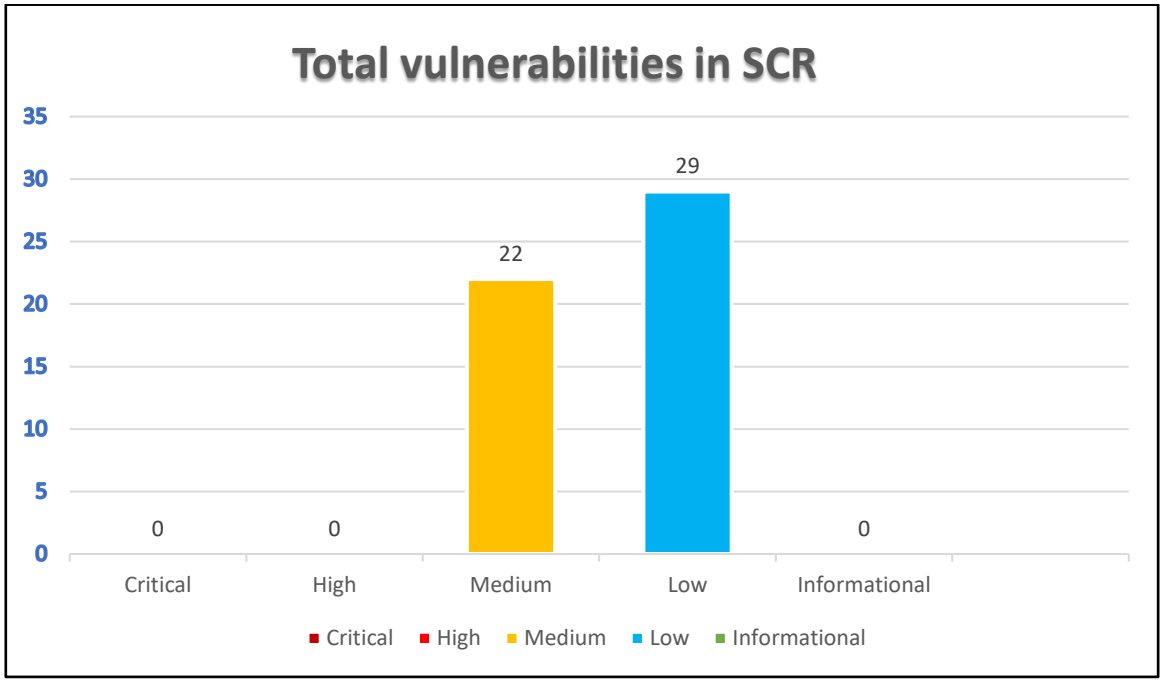
Number of applications	Total Vulnerabilities					
	Critical	High	Medium	Low	Info	Total
1	0	0	22	29	0	51

The below table summarizes the list of vulnerabilities with corresponding risk ratings.

SL. No.	Vulnerability Name	Severity Rating
1	Command Injection	Medium
2	Credential Management: Hardcoded Api	Medium
3	Cross-Site Scripting: DOM	Medium
4	Insecure SSL: Server Identity Verification Disabled	Medium
5	Insecure Transport: Mail Transmission	Medium
6	Insecure Transport: Weak SSL Protocol	Medium
7	Path Manipulation	Medium
8	Privacy Violation	Medium
9	Weak Encryption	Medium
10	Asp.Net MVC Bad Practices: Model With Required Non-Nullable Property	Medium
11	Cross-Site Scripting: Reflected	Medium
12	Dynamic Code Evaluation: Code Injection	Medium
13	Insecure Randomness	Medium
14	Key Management: Hardcoded PBE Password	Medium
15	Password Management: Empty Password	Medium
16	Password Management: Hardcoded Password	Medium
17	Privacy Violation: Heap Inspection	Medium
18	Process Control	Medium
19	Server-Side Request Forgery	Medium
20	Weak Encryption: Insecure Mode Of Operation	Medium
21	XML Injection	Medium
22	XPath Injection	Medium
23	Path Manipulation: Base Path Overwriting	Low
24	Path Manipulation: Zip Entry Overwrite	Low
25	System Information Leak: External	Low
26	WCF Misconfiguration: Anonymous Transport Client	Low
27	WCF Misconfiguration: Insufficient Logging	Low
28	WCF Misconfiguration: Service Enumeration	Low
29	WCF Misconfiguration: Weak Token	Low
30	Denial Of Service	Low
31	Denial Of Service: Regular Expression	Low

32	Header Manipulation	Low
33	Missing Xml Validation	Low
34	Often Misused: Authentication	Low
35	Password Management: Lack Of Key Derivation Function	Low
36	Password Management: Null Password	Low
37	Password Management: Password In Comment	Low
38	Poor Logging Practice: Use Of A System Output Stream	Low
39	Resource Injection	Low
40	Setting Manipulation	Low
41	System Information Leak	Low
42	System Information Leak: Internal	Low
43	Unchecked Return Value	Low
44	Unsafe Native Invoke	Low
45	Unsafe Reflection	Low
46	WCF Misconfiguration: Throttling Not Enabled	Low
47	Weak Cryptographic Hash	Low
48	Weak Cryptographic Hash: Insecure PBE Iteration Count	Low
49	Weak Cryptographic Hash: User-Controlled PBE Salt	Low
50	Weak Xml Schema: Type Any	Low
51	Weak Xml Schema: Unbounded Occurrences	Low

GRAPHICAL PRESENTATION



CYBERPWN
EMPOWERING CYBER RESILIENCE

RESULT OVERVIEW SOURCE COMPOSITION ANALYSIS

The following table summarizes the list of findings discovered in **Source Composition Analysis** and their identified risk:

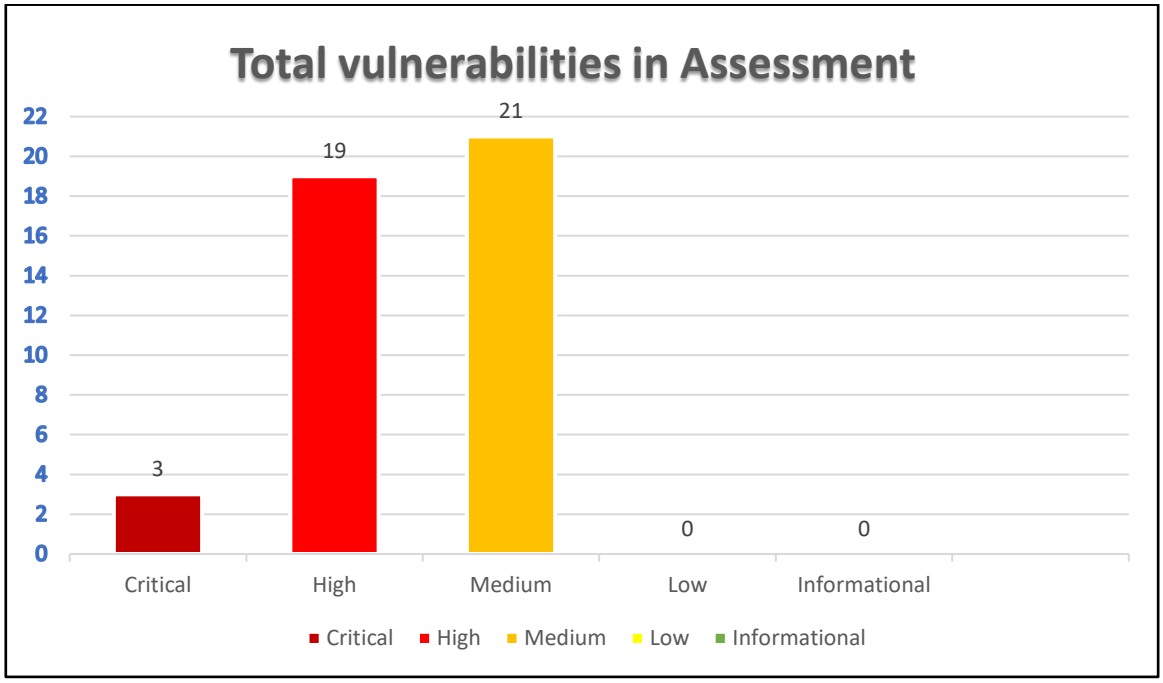
Number of applications	Total Vulnerabilities					
	Critical	High	Medium	Low	Info	Total
1	3	19	21	0	0	43

The below table summarizes the list of vulnerabilities with corresponding risk ratings.

SL. No.	Vulnerability Name	Severity Rating
1	Heap-based Buffer Overflow	Critical
2	Integer Overflow or Wraparound	Critical
3	Out-of-bounds Write	Critical
4	Use of Externally-Controlled Format String	High
5	Release of Invalid Pointer or Reference	High
6	NULL Pointer Dereference	High
7	Stack-based Buffer Overflow	High
8	Off-by-one Error	High
9	Allocation of Resources Without Limits or Throttling	High
10	Directory Traversal	High
11	Time-of-check Time-of-use (TOCTOU) Race Condition	High
12	Access of Uninitialized Pointer	High
13	Uncontrolled Recursion	High
14	Use After Free	High
15	Denial of Service (DoS)	High
16	Infinite loop	High
17	XML External Entity (XXE) Injection	High
18	Insecure Defaults	High
19	Improper Certificate Validation	High
20	Privilege Escalation	High
21	Information Exposure	High
22	Out-of-bounds Read	High
23	Authentication Bypass	Medium
24	CRLF Injection	Medium
25	Resource Injection	Medium
26	Insertion of Sensitive Information into Log File	Medium
27	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	Medium
28	Arbitrary Code Injection	Medium
29	Missing Release of Resource after Effective Lifetime	Medium
30	Incomplete List of Disallowed Inputs	Medium
31	Unchecked Input for Loop Condition	Medium

32	Missing Release of Memory after Effective Lifetime	Medium
33	Expired Pointer Dereference	Medium
34	Integer Underflow (Wrap or Wraparound)	Medium
35	Improper Validation of Array Index	Medium
36	Insecure Randomness	Medium
37	Unsynchronized Access to Shared Data in a Multithreaded Context	Medium
38	Improper Authentication	Medium
39	Incorrect Calculation of Buffer Size	Medium
40	Buffer Access with Incorrect Length Value	Medium
41	Division by zero	Medium
42	Buffer Over-read	Medium
43	Improper Encoding or Escaping of Output	Medium

GRAPHICAL PRESENTATION



VULNERABILITIES DETAILS

1. COMMAND INJECTION	
Source File	RobilityDesigner/Functions/SmartSpy/MainWindow.xaml.cs; 149 RobilityDesigner/Python/Lib/site-packages/pip/_internal/commands/configuration.py; 239 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/_msvccompiler.py; 85 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/spawn.py; 57 RobilityDesigner/Python/Lib/site-packages/setuptools/msvc.py; 96 RobilityDesigner/Robility.AuthSystem/Program.cs; 136 RobilityDesigner/Robility.Launcher/ViewModel/ConnectFormViewModel.cs; 487 RobilityDesigner/ViewModel/MainWindwoActiproViewModel.cs; 5175 RobilityDesigner/ViewModel/SupportPublish/PublishCommon.cs; 234 RobilityDesigner/Functions/ExecuteXamlWorkflow/WPFMessageBox.xaml.cs; 154 RobilityDesigner/Functions/GitLeaksScannerLib/GitLeaksScanner.cs; 284, 294 RobilityDesigner/Functions/ProductUpdater/View/WPFMessageBox.xaml.cs; 152 RobilityDesigner/Functions/ProductUpdater/ViewModel/ProductUpdateViewModel.cs; 334 RobilityDesigner/Functions/Robility.Product.Update/ProductUpdate.cs; 416 RobilityDesigner/Functions/RobilityUpdater/Models/Restore.cs; 218 RobilityDesigner/Functions/RobilityUpdater/Models/Updater.cs; 224 RobilityDesigner/Functions/SmartRPAActivities/RobotFunctions.cs; 754, 758 RobilityDesigner/Robility.Launcher/Launcher/AppControl.xaml.cs; 128 RobilityDesigner/Robility.Launcher/ViewModel/ApplicationMenu.xaml.cs; 172 RobilityDesigner/Robility.Launcher/ViewModel/ConnectFormViewModel.cs; 485 RobilityDesigner/Robility.Launcher/Views/ConnectForm.xaml.cs; 30 RobilityDesigner/Robility.Launcher/Views/DesignerMenuControl.xaml.cs; 174 RobilityDesigner/Robility.Launcher/Views/MarketPlaceDownload.xaml.cs; 105, 112 RobilityDesigner/Robility.Launcher/Views/RobilityLauncher.xaml.cs; 185 RobilityDesigner/Robility.Launcher/Views/SupportClasses/HandleExpiredLicense.cs; 43 RobilityDesigner/Robility.Launcher/Views/WPFMessageBox.xaml.cs; 224 RobilityDesigner/ViewModel/FormBuilderInstall.cs; 81, 179 RobilityDesigner/ViewModel/MainWindwoActiproViewModel.cs; 5539, 6930 RobilityDesigner/ViewModel/SupportPublish/PublishCommon.cs; 233 RobilityDesigner/Views/WPFMessageBox.xaml.cs; 224 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/commands/configuration.py; 239 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/_msvccompiler.py; 85 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/msvc9compiler.py; 284

	Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/spawn.py; 57 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/msvc.py; 96 Runner/SmartRPALogonService/LogonClass/AutoLogon.cs; 155 RobilityActivites/ModernDesktopExecutorLib/Utilities/LaunchUwpApps.cs; 41 RobilityActivites/Robility.CoreActivities/InvokeVBScript.cs; 106 RobilityActivites/Robility.CoreActivities/StartProcessHelper .cs; 144 RobilityActivites/Robility.DesktopAutomation/Utilities/LaunchUwpApps.cs; 41 RobilityActivites/Robility.ModernDesktopAutomation/OpenSpyApplication.cs; 101 RobilityActivites/Robility.SAPAutomation/ScriptExecutor.cs; 37 RobilityActivites/Robility.SQliteAutomation/DBBackup.cs; 196 RobilityActivites/Robility.SQliteAutomation/ExportCSV.cs; 222 RobilityActivites/ChromeSpy - Copy/MainWindow.xaml.cs; 219, 223, 227 RobilityActivites/ChromeSpy - Copy/View/AdvancedSpyWindow.xaml.cs; 178, 182, 186 RobilityActivites/ChromeSpy - Copy/View/SpyWindow.xaml.cs; 173, 177, 181 RobilityActivites/ChromeSpy/MainWindow.xaml.cs; 288, 292, 296 RobilityActivites/ChromeSpy/View/AdvancedSpyWindow.xaml.cs; 178, 182, 186 RobilityActivites/ChromeSpy/View/SpyWindow.xaml.cs; 173, 177, 181 RobilityActivites/FlaUInspect/ViewModels/MainViewModel.cs; 47 RobilityActivites/GlobalElementEditor/Helper/DesignEvents.cs; 38, 78 RobilityActivites/GlobalElementEditor/Views/ElementEditor.xaml.cs; 250, 254 RobilityActivites/JavaAppExecutorLib/UiActionStarter.cs; 136, 138 RobilityActivites/ModernDesktopExecutorLib/UiActionStarter.cs; 138, 140 RobilityActivites/ModernDesktopSpy/ViewModels/MainViewModel.cs; 86 RobilityActivites/Robility.AdvancedWebAutomation/OpenWebBrowser.cs; 149, 152, 155, 162, 165, 168, 175, 178, 181 RobilityActivites/Robility.AppIntegration/UserControl/ConnectorHelper.cs; 155 RobilityActivites/Robility.AssistedVirtualSession/Utilities/Common.cs; 61, 62 RobilityActivites/Robility.AzureKeyvault/Common.cs; 122, 124 RobilityActivites/Robility.Cognitive/ImageOptimization.cs; 55 RobilityActivites/Robility.CopilotControl/ViewModel/ValidationNotificationViewModel.cs; 98 RobilityActivites/Robility.CoreActivities.Tests/KillProcessTests.cs; 85, 95 RobilityActivites/Robility.CoreActivities/StartProcessHelper .cs; 132, 133 RobilityActivites/Robility.DesktopAutomation/Designer/DsMouseHover.xaml.cs; 83 RobilityActivites/Robility.DesktopAutomation/Designer/DsSelectValue.xaml.cs; 97 RobilityActivites/Robility.DesktopAutomation/Designer/DsSetText.xaml.cs; 160 RobilityActivites/Robility.DesktopAutomation/Designer/dsClickEvent.xaml.cs; 150, 166 RobilityActivites/Robility.DesktopAutomation/Designer/dsElementExist.xaml.cs; 130, 157 RobilityActivites/Robility.DesktopAutomation/Editor/SelecterEditor.xaml.cs; 263 RobilityActivites/Robility.DesktopAutomation/Utilities/SelecterEditor.xaml.cs; 215

	RobilityActivites/Robility.DesktopAutomationUIA3/OpenSpyApplication.cs; 57, 61 RobilityActivites/Robility.DesktopAutomationUIA3/Utilities/Common.cs; 140, 142 RobilityActivites/Robility.DesktopAutomation_Production/OpenApps.cs; 104 RobilityActivites/Robility.GenAI/Common/StartProcess.cs; 38, 39 RobilityActivites/Robility.GoogleCognitiveServices/VisionOCR.cs; 758 RobilityActivites/Robility.InternetExplorer/Designer/DsGetText.xaml.cs; 84, 118 RobilityActivites/Robility.InternetExplorer/Designer/DsHTMLTableToDataTable.xaml.cs; 84, 118 RobilityActivites/Robility.InternetExplorer/Designer/DsMouseHover.xaml.cs; 83, 117 RobilityActivites/Robility.InternetExplorer/Designer/DsSelectValue.xaml.cs; 59, 94 RobilityActivites/Robility.InternetExplorer/Designer/DsSetText.xaml.cs; 86, 120 RobilityActivites/Robility.InternetExplorer/Designer/dsClickEvent.xaml.cs; 85, 119 RobilityActivites/Robility.InternetExplorer/Designer/dsElementExist.xaml.cs; 83, 117 RobilityActivites/Robility.InternetExplorer/Designer/dsGetAttributes.xaml.cs; 101 RobilityActivites/Robility.Invoke/WPFMessageBox.xaml.cs; 154 RobilityActivites/Robility.JavaApp/LaunchJavaApplication.cs; 105, 106 RobilityActivites/Robility.JavaApp/OpenSpyApplication.cs; 53, 84 RobilityActivites/Robility.Marketplace/PythonScriptLoader.cs; 427, 428 RobilityActivites/Robility.Marketplace/PythonVirtualEnvironement.cs; 158 RobilityActivites/Robility.MicrosoftCognitiveServices/ImageOptimization.cs; 55 RobilityActivites/Robility.ModernDesktopAutomation/OpenSpyApplication.cs; 56 RobilityActivites/Robility.NLTKEntityextraction/NLTKNamedentityExtraction.cs; 115 RobilityActivites/Robility.PythonAutomation/InvokeScript.cs; 30 RobilityActivites/Robility.SAPAutomation/SapInvoke.cs; 92 RobilityActivites/Robility.SQliteAutomation/ImportData.cs; 1053 RobilityActivites/Robility.ScreenRecording/Utilities.cs; 145, 147 RobilityActivites/Robility.SmartRPACognitiveServices/ImageOptimization.cs; 71 RobilityActivites/Robility.Terminal/Common/ConnectNamedPipe.cs; 131, 134 RobilityActivites/Robility.Terminal/TerminalClass/TerminalConnection.cs; 52 RobilityActivites/Robility.WebAutomation/OpenWebBrowser.cs; 101, 104, 107, 114, 117, 120, 127, 130, 133 RobilityActivites/Robility.WebAutomation_V3/OpenWebBrowser.cs; 186, 188 RobilityActivites/SpyCommunicator/CommonMethods/DesignEvents.cs; 352, 390
Observation	During assessment it was observed that the mentioned method calls Start() to execute a command built from untrusted data. This call can cause the program to execute malicious commands on behalf of an attacker.
Severity Rating	**Medium**
Impact	Command injection vulnerabilities take two forms: - An attacker can change the command that the program executes: the attacker explicitly controls what the command is. - An attacker can change the environment in which the command executes: the attacker implicitly controls what the command means.

Recommendation	It is recommended to not allow users to have direct control over the commands executed by the program.
References	https://vulncat.fortify.com/en/detail?category=Command+Injection

Proof of Concept:

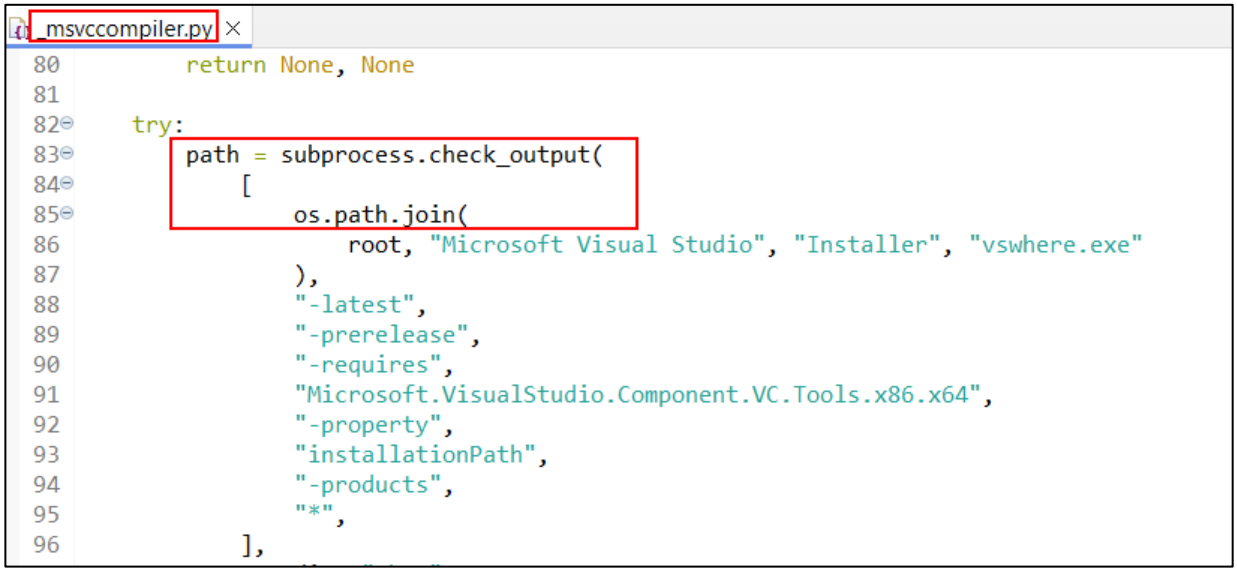


FIGURE 1: COMMAND INJECTION

2. CREDENTIAL MANAGEMENT: HARDCODED API CREDENTIALS	
Source File	RobilityDesigner/Pipeline/Development/RobilityDesigner_App-Development.yml; 192 RobilityDesigner/Pipeline/SonarQube/RobilityDesigner-App-SQ-Dev.yml; 59 RobilityActivites/Pipeline/SonarQube/RobilityWebClient-SQ.yml; 53 RobilityActivites/Pipeline/SonarQube/RobilityWordDocument-SQ.yml; 53 RobilityActivites/Pipeline/SonarQube/Robility_ActiveDirectory-SQ.yml; 50 RobilityActivites/Pipeline/SonarQube/Robility_AmazonRekognition-SQ.yml; 50 RobilityActivites/Pipeline/SonarQube/Robility_AmazonS3-SQ.yml; 50 RobilityActivites/Pipeline/SonarQube/Robility_AssistedVirtualSession-SQ.yml; 50 RobilityActivites/Pipeline/SonarQube/Robility_AylienEntityExtraction-SQ.yml; 50 RobilityActivites/Pipeline/SonarQube/Robility_AzureAIFormRecognizer-SQ.yml; 50 RobilityActivites/Pipeline/SonarQube/Robility_EmailAutomation_Outlook-SQ.yml; 63 RobilityActivites/Pipeline/SonarQube/Robility_WebAutomation_V3-SQ.yml; 63 RobilityActivites/Robility.AzureStorage/Designer/DesignerAzureScope.xaml.cs; 162 RobilityActivites/Robility.AzureStorage/app.config; 4 RobilityActivites/Robility.CoreActivities/GitLeaks/gitleaks.toml; 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583 RobilityActivites/Robility.Manager.Tests/BusinessLayer/SetAssetExecutionTests.cs; 53, 92 RobilityActivites/Robility.MicrosoftOutlook365/MoveEmail.cs; 188 RobilityActivites/Robility.UIVision/Common/ClsConstVariable.cs; 46 RobilityActivites/Robility.UIVision/Properties/Resources.Designer.cs; 91 RobilityActivites/Robility.UIVision/Properties/Resources.resx; 130 Runner/Pipeline/Staging/Runner7App-Pipeline.yml; 190
Observation	During assessment it was observed that application is vulnerable to Credential Management: Hardcoded API Credentials. Hardcoded API credentials can compromise system security.
Severity Rating	**Medium**
Impact	Never hardcode credentials, including usernames, passwords, API keys, API secrets, and API Tokens. Not only are hardcoded credentials visible to all of the project developers, they are extremely difficult to update. After the code is in production, the credentials cannot be changed without patching the software. If the credentials are compromised, the organization must choose between security and system availability.
Recommendation	Make sure that API credentials are either loaded from a configuration file that is only available in the runtime environment or from environment variables.
References	https://vulncat.fortify.com/en/detail?category=Credential+Management&subcategory=Hardcoded+API+Credentials
Proof of Concept:	

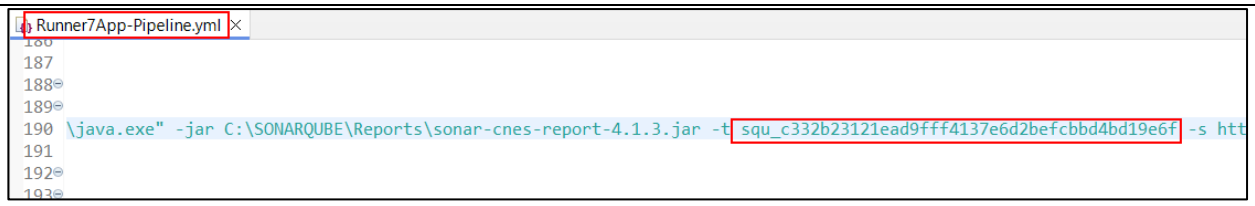


FIGURE 2: CREDENTIAL MANAGEMENT: HARDCODED API CREDENTIALS

3. CROSS-SITE SCRIPTING: DOM	
Source File	RobilityDesigner/Functions/RobilityChromeNativeApp/RuntimeScript/runtimeScript.js; 1025 RobilityDesigner/Functions/RobilityEdgeNativeApp/RuntimeScript/runtimeScript.js; 1026 RobilityActivites/Robility.WebAutomation/Js/CursorIframeMove_18112022.js; 1134 RobilityActivites/Robility.WebAutomation/Js/Cursor_NstIframeBugFix_V7_17112022.js; 1134 RobilityActivites/Robility.WebAutomation/Js/Live_latest_runtimeScript_17112022.js; 1114 RobilityActivites/Robility.WebAutomation/Js/runtimeScript_Minify_21112022 .js; 519 RobilityActivites/Robility.WebAutomation_V3/Js/CursorIframeMove_18112022.js; 1134 RobilityActivites/Robility.WebAutomation_V3/Js/Cursor_NstIframeBugFix_V7_17112022.js; 1134 RobilityActivites/Robility.WebAutomation_V3/Js/Live_latest_runtimeScript_17112022.js; 1114 RobilityActivites/Robility.WebAutomation_V3/Js/runtimeScript_Minify_21112022 .js; 519 RobilityActivites/Robility.WebAutomation_V3/Js/runtimeScript_V3_01052022.js; 1225 RobilityActivites/Robility.WebAutomation_V3/Plugin/ManifestV3/lgnoojafhdgcpllpgolgpmjjdejnneom/Plain/3.1/runtimeScript.js; 1296, 1334 RobilityActivites/Robility.WebAutomation_V3/Plugin/ManifestV3/lgnoojafhdgcpllpgolgpmjjdejnneom/Plain/3.4/runtimeScript.js; 745, 781 RobilityActivites/Robility.WebAutomation_V3/Plugin/ManifestV3/lgnoojafhdgcpllpgolgpmjjdejnneom/Plain/3.5/runtimeScript.js; 789, 825 RobilityActivites/Robility.WebAutomation_V3/Plugin/ManifestV3/lgnoojafhdgcpllpgolgpmjjdejnneom/Plain/3.6/runtimeScript.js; 789, 825 RobilityActivites/Robility.WebAutomation_V3/Plugin/ManifestV3/lgnoojafhdgcpllpgolgpmjjdejnneom/Plain/3.7/runtimeScript.js; 789, 825 RobilityActivites/Robility.WebAutomation_V3/Plugin/ManifestV3/lgnoojafhdgcpllpgolgpmjjdejnneom/Plain/3.8/runtimeScript.js; 1072, 1108 RobilityActivites/Robility.WebAutomation_V3/Plugin/ManifestV3/lgnoojafhdgcpllpgolgpmjjdejnneom/Plain/3.9/runtimeScript.js; 1169, 1205 RobilityActivites/lbmeghcehlmclgjmnefeflchpbdblamd/RuntimeScript/runtimeScript.js; 1021 Runner/RobilityRunner/Robility7/Chrome/RuntimeScript/runtimeScript.js; 1025 Runner/RobilityRunner/Robility7/Edge/RuntimeScript/runtimeScript.js; 1026
Observation	During assessment it was observed that the method sends unvalidated data to a web browser, which can result in the browser executing malicious code.
Severity Rating	**Medium**

Impact	The malicious content sent to the web browser often takes the form of a JavaScript segment, but can also include HTML, Flash or any other type of code that the browser executes. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data such as cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.
Recommendation	It is recommended to ensure that validation occurs in the required places and that relevant properties are set to prevent vulnerabilities.
References	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496719#9

Proof of Concept:

runtimeScript.js

```
1022 function CloseTab() {
1023     var result;
1024     try {
1025         var objWindow = window.open(location.href, "_self");
1026         objWindow.close();
1027         result = {
1028             Status: true,
1029             Message: 'Successfully tab closed.'
1030         };
```

FIGURE 3: CROSS-SITE SCRIPTING: DOM

4. INSECURE SSL: SERVER IDENTITY VERIFICATION DISABLED

Source File	RobilityDesigner/Python/Lib/site-packages/setuptools/config/_validate_pyproject/formats.py; 123 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/config/_validate_pyproject/formats.py; 123 RobilityActivites/RobilityWebClient/RestConsumerPartial.cs; 35
Observation	During assessment it was observed that the connection established does not verify the server certificate when making an SSL connection. This leaves the application vulnerable to a man-in-the-middle attack.
Severity Rating	**Medium**
Impact	In some libraries that use SSL connections, the server certificate is not verified by default. This is equivalent to trusting all certificates. In other instances, this is can be explicitly disabled, whether by intention or not.
Recommendation	It is recommended to not forget proper server verification checks when making SSL connections. Depending on the library used, make sure to verify server identity and establish a secure SSL connection.
References	https://vulncat.fortify.com/en/detail?category=Insecure+SSL&subcategory=Server+Identity+Verification+Disabled

Proof of Concept:

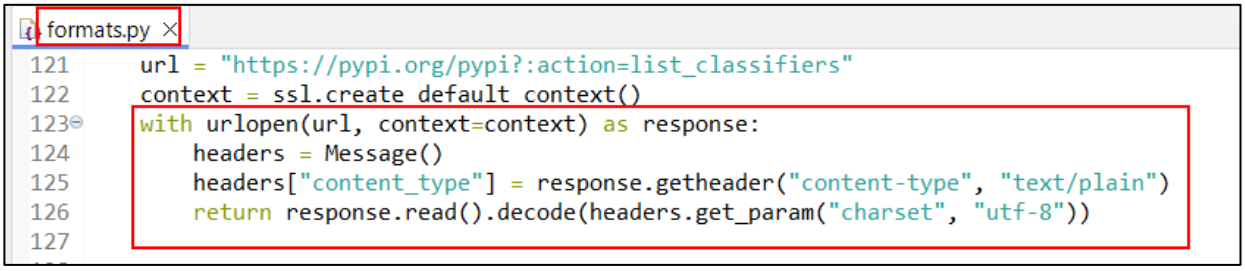


FIGURE 4: INSECURE SSL: SERVER IDENTITY VERIFICATION DISABLED

5. INSECURE TRANSPORT: MAIL TRANSMISSION

Source File	RobilityActivites/Robility.MailAutomation.Outlook/Send.cs; 205
Observation	During assessment it was observed that the mentioned establishes an unencrypted connection to a mail server allowing an attacker to carry out a man-in-the-middle attack and read all the mail transmissions.
Severity Rating	**Medium**
Impact	Sensitive data sent over the wire unencrypted is subject to be read/modified by any attacker that can intercept the network traffic.
Recommendation	It is recommended to use encrypted alternatives on different ports that use SSL/TLS to encrypt all the data being sent over the wire or to upgrade an existing unencrypted connection to SSL/TLS. Always use these alternatives when possible.
References	https://vulncat.fortify.com/en/detail?category=Insecure+Transport&subcategory=Mail+Transmission

Proof of Concept:



FIGURE 5: INSECURE TRANSPORT: MAIL TRANSMISSION

6. INSECURE TRANSPORT: WEAK SSL PROTOCOL	
Source File	RobilityDesigner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 1435 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 1435 RobilityActivites/Robility.AzureAIFormRecognizer/AnalyzeBusinessCards.cs; 111 RobilityActivites/Robility.AzureAIFormRecognizer/AnalyzeCustomForms.cs; 111 RobilityActivites/Robility.AzureAIFormRecognizer/AnalyzeLayouts.cs; 111 RobilityActivites/Robility.AzureAIFormRecognizer/AnalyzeReceipts.cs; 111 RobilityActivites/Robility.AzureAIFormRecognizer/GetModelInfo.cs; 79 RobilityActivites/Robility.AzureAIFormRecognizer/TrainModel.cs; 101 RobilityActivites/Robility.MicrosoftEntityExtraction/Robility.MicrosoftEntityExtraction/RecognizeEntitiesSample.cs; 18 RobilityActivites/Robility.MicrosoftEntityExtraction/SmartRPA.Activities.MicrosoftEntityExtraction/RecognizeEntitiesSample.cs; 18
Observation	During assessment it was observed that the mentioned establishes an unencrypted connection to a mail server allowing an attacker to carry out a man-in-the-middle attack and read all the mail transmissions.
Severity Rating	**Medium**
Impact	Sensitive data sent over the wire unencrypted is subject to be read/modified by any attacker that can intercept the network traffic.
Recommendation	It is recommended to use encrypted alternatives on different ports that use SSL/TLS to encrypt all the data being sent over the wire or to upgrade an existing unencrypted connection to SSL/TLS. Always use these alternatives when possible.
References	https://vulncat.fortify.com/en/detail?category=Insecure+Transport&subcategory=Mail+Transmission

Proof of Concept:

util.py

```
1433                self._tunnel()
1434
1435            context = ssl.SSLContext(ssl.PROTOCOL_SSLv23)
1436            if hasattr(ssl, 'OP_NO_SSLv2'):
1437                context.options |= ssl.OP_NO_SSLv2
1438            if self.cert_file:
1439                context.load_cert_chain(self.cert_file, self.key_file)
```

FIGURE 6: INSECURE TRANSPORT: MAIL TRANSMISSION

7. PATH MANIPULATION

Source File	RobilityDesigner/Python/Lib/site-packages/setuptools/package_index.py; 389 RobilityDesigner/ChildSessionRunnerInstance/WorkflowExecution/Runner.cs; 101 RobilityDesigner/DllManagement/DynamicDllManagement.cs; 33, 40, 71, 102, 208 RobilityDesigner/Functions/ControlListView/TileListItem.cs; 1016, 1074, 1091, 1169, 1297, 1302, 1509, 1560, 1565, 1631 RobilityDesigner/Functions/ExecuteXamlWorkflow/BindDllMethods.cs; 38 RobilityDesigner/Functions/ExecuteXamlWorkflow/ExecuteXamlWorkflowDesigner.xaml.cs; 306, 670 RobilityDesigner/Functions/ExecuteXamlWorkflow/TemplatesValidation.cs; 49, 114, 188, 189, 328, 362, 395, 399, 411, 415, 454, 630, 636, 651, 654, 661, 700, 787 RobilityDesigner/Functions/FeatureManager/Features.cs; 444, 447, 843 RobilityDesigner/Functions/ProjectSolution/ProjectManager/ProjectManager.cs; 44, 51, 58, 67, 78, 333 RobilityDesigner/Functions/Robility.DebugTracking/VisualTracking.cs; 614 RobilityDesigner/Functions/Robility.RemoveUnused/RemoveUnusedDependencies.cs; 41 RobilityDesigner/Functions/Robility.ServiceCall/ServiceCalls.cs; 200 RobilityDesigner/Functions/Robility.WorkflowAnalyzer/Helpers/RulesHelper.cs; 39 RobilityDesigner/Functions/Robility.WorkflowAnalyzer/Validate/FindStopStatus.cs; 301 RobilityDesigner/Functions/Robility.WorkflowAnalyzer/Validate/WorkflowHelper.cs; 64, 87 RobilityDesigner/Functions/SmartRPAActivities/TemplateCommonMethods.cs; 417, 422, 664, 667 RobilityDesigner/ManageFeatures/ManageFeatureViewModel.cs; 1259 RobilityDesigner/ObjectRepository/RespositoryParser.cs; 38, 64, 72 RobilityDesigner/Prompt/ClsPromptJsonManage.cs; 39, 67 RobilityDesigner/Prompt/PromptTree.cs; 35, 38, 47, 68 RobilityDesigner/Prompt/PromptWindow.cs; 126, 141, 154, 159, 195 RobilityDesigner/Python/Lib/site-packages/PIL/IcnsImagePlugin.py; 391 RobilityDesigner/Python/Lib/site-packages/PIL/Image.py; 2419 RobilityDesigner/Python/Lib/site-packages/PIL/ImageFile.py; 105 RobilityDesigner/Python/Lib/site-packages/PIL/ImageFont.py; 822 RobilityDesigner/Python/Lib/site-packages/PIL/SpiderImagePlugin.py; 83 RobilityDesigner/Python/Lib/site-packages/pip/_internal/operations/install/wheel.py; 390 RobilityDesigner/Python/Lib/site-packages/pip/_internal/utils/unpacking.py; 115, 140, 218 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/cachecontrol/caches/file_cache.py; 52 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/distlib/compat.py; 221 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 546

	RobilityDesigner/Python/Lib/site-packages/pip/_vendor/pkg_resources/__init__.py; 1896, 1906, 1907, 1929, 3251 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/pygments/formatters/img.py; 128 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/pyproject_hooks/_in_process/_in_process.py; 31, 36 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/rich/console.py; 2275 RobilityDesigner/Python/Lib/site-packages/pkg_resources/__init__.py; 1896, 1906, 1907, 1929, 3251 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/config.py; 44 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/file_util.py; 27, 33, 40, 149, 158, 172, 212, 225, 229, 243 RobilityDesigner/Python/Lib/site-packages/setuptools/command/build_ext.py; 298, 341 RobilityDesigner/Python/Lib/site-packages/setuptools/wheel.py; 228, 230 RobilityDesigner/ReusableObjects/ViewModel/ReusableObjectViewModel.cs; 338, 356, 911, 955 RobilityDesigner/Robility.Launcher/App.xaml.cs; 159 RobilityDesigner/Robility.Launcher/ManageFeatures/ManageFeatureViewModel.cs; 2442, 2620, 3010, 3029, 3186, 3191, 3196, 3198, 3389, 3393, 3399, 3414, 3760, 3766 RobilityDesigner/Robility.Launcher/ManageFeatures/Validatefeaturedlls.cs; 79 RobilityDesigner/Robility.Launcher/ViewModel/Advancedspyenableandwritesolutionjson.cs; 24, 30, 44, 67, 124 RobilityDesigner/Robility.Launcher/ViewModel/Assign/DefaultAssign.cs; 47 RobilityDesigner/Robility.Launcher/ViewModel/DesignerLauncherViewModel.cs; 1867, 2219, 2228, 2240, 3268, 3401, 4101, 5278, 5283 RobilityDesigner/Robility.Launcher/ViewModel/FileUtility.cs; 60, 62, 109, 138 RobilityDesigner/Robility.Launcher/ViewModel/OpenSolution/RenameSolution.cs; 228, 265 RobilityDesigner/Robility.Launcher/ViewModel/UpdateFeatures.cs; 399, 440, 451, 498 RobilityDesigner/Robility.Launcher/Views/NewProject.xaml.cs; 124, 131 RobilityDesigner/Robility.Launcher/Views/NewTemplate.xaml.cs; 121 RobilityDesigner/Robility.Launcher/Views/NewWorkflow.xaml.cs; 208 RobilityDesigner/RobilityRoboPoster/RobilityRoboPoster/PublishSolution.cs; 120 RobilityDesigner/RobilityRunner/Program.cs; 147 RobilityDesigner/RobilityRunner/WorkflowExecution/Runner.cs; 653 RobilityDesigner/RunnerExecution/RunnerInstanceExecution.cs; 458, 556 RobilityDesigner/RunnerInstance/WorkflowExecution/Runner.cs; 882 RobilityDesigner/TreeViewToolBox/AddTemplateFolder.cs; 136 RobilityDesigner/TreeViewToolBox/TemplateFolderManager.cs; 35 RobilityDesigner/TreeViewToolBox/TreeviewToolbox.cs; 898, 921, 995, 1050 RobilityDesigner/UIExplore/PluginsHandlers/BrowserSpyCommunicator.cs; 62

	RobilityDesigner/Utilities/ModelItemUpdateUtility.cs; 123 RobilityDesigner/ViewModel/AddWorkflowDependencies.cs; 59, 140 RobilityDesigner/ViewModel/DependencyVersionViewModel.cs; 92, 94 RobilityDesigner/ViewModel/DllImports.cs; 195, 328, 334, 337, 448, 493, 516, 633, 696, 699, 708, 732, 749, 880, 909, 934, 962, 987 RobilityDesigner/ViewModel/ImportWorkflow/ImportFeaturesDetails.cs; 29 RobilityDesigner/ViewModel/Importfiles.cs; 251, 267, 277, 284, 296, 314, 317, 326, 346, 372, 382, 495, 532, 621, 674, 686 RobilityDesigner/ViewModel/InteractActivityFunctions.cs; 149, 238 RobilityDesigner/ViewModel/InvokeTemplateArguments.cs; 37, 39, 54, 60 RobilityDesigner/ViewModel/MainWindwoActiproViewModel.cs; 1317, 3560, 3782, 3788, 4151, 4720, 5195, 5208, 5232, 5252, 5269, 5358, 5423, 5429, 6944, 7073 RobilityDesigner/ViewModel/PublishProjectDetails.cs; 384, 426 RobilityDesigner/ViewModel/PublishSolutionToManager.cs; 202, 316, 363, 432, 479 RobilityDesigner/ViewModel/RemoveUnusedWorkflows.cs; 162, 290 RobilityDesigner/ViewModel/RenameFolder.cs; 127, 144, 201 RobilityDesigner/ViewModel/SolutionProperties.cs; 49, 125 RobilityDesigner/ViewModel/SolutionPropertiescontextmenus.cs; 1018, 1076, 1251, 1255, 1262, 1266, 1336, 1432, 1449, 1566, 1622, 1682, 1692, 1724, 1731, 1764, 1785, 1815, 1839, 1860, 1890, 1917, 1924, 1983, 2046, 2074 RobilityDesigner/ViewModel/SupportPublish/PublishCommon.cs; 82 RobilityDesigner/ViewModel/SupportPublish/PublishObjectHelper.cs; 43 RobilityDesigner/ViewModel/UpdateDisplyInfo.cs; 31, 82 RobilityDesigner/ViewModel/WorkflowExecution.cs; 620, 851, 875, 902, 912, 1491, 1495, 1532, 1546, 1588, 1602 RobilityDesigner/ViewModel/WorkflowViewModel.cs; 196, 256, 265, 285, 296, 858, 872, 879, 914, 959 RobilityDesigner/Views/ProjectProperties.xaml.cs; 61, 165, 169 RobilityDesigner/Views/PublishProject.xaml.cs; 206, 458, 462 RobilityDesigner/WorkFlowScan/FolderHasher.cs; 38, 41, 80, 83, 98, 172, 180, 250, 265, 281, 371 RobilityDesigner/WorkFlowScan/LogCleaner.cs; 40, 44 RobilityDesigner/WorkFlowScan/PromptSecurityScan.cs; 43 RobilityDesigner/WorkFlowScan/SecurityLogHelper.cs; 37, 44, 57, 59, 67, 179, 202, 210, 213, 223, 225 RobilityDesigner/WorkFlowScan/WorkFlowScanTreeView.cs; 60 RobilityDesigner/WorkflowAnalyzer/AddWorkflowEntry.cs; 60 RobilityDesigner/WorkflowAnalyzer/Analyzer.cs; 494 RobilityDesigner/WorkflowAnalyzer/RestrictPublish.cs; 70 RobilityDesigner/WorkflowAnalyzer/SaveReportData.cs; 54, 58, 88, 123, 185, 202, 271 RobilityDesigner/WorkflowAnalyzer/WorkflowAnalyzerTreeView.cs; 280 RobilityDesigner/DllManagement/DynamicDllManagement.cs; 31, 206

	RobilityDesigner/Functions/ControlListView/TileListItem.cs; 674, 1007, 1009, 1011, 1072, 1089, 1141, 1377, 1402, 1501, 1503, 1505, 1558, 1563, 1605 RobilityDesigner/Functions/ExecuteXamlWorkflow/ExecuteXamlWorkflowDesigner.xaml.cs; 522 RobilityDesigner/Functions/ExecuteXamlWorkflow/InvokeDll.cs; 97 RobilityDesigner/Functions/ExecuteXamlWorkflow/TemplatesValidation.cs; 388, 393, 397, 409, 413, 628, 633 RobilityDesigner/Functions/FeatureManager/Features.cs; 439, 837 RobilityDesigner/Functions/GitLeaksScannerLib/GitLeaksScanner.cs; 73, 77 RobilityDesigner/Functions/Robility.DebugTracking/VisualTracking.cs; 612 RobilityDesigner/Functions/Robility.RemoveUnused/RemoveUnusedDependencies.cs; 36 RobilityDesigner/Functions/Robility.ServiceCall/ServiceCalls.cs; 198 RobilityDesigner/Functions/Robility.WorkflowAnalyzer/Helpers/RulesHelper.cs; 34 RobilityDesigner/Functions/SmartRPAActivities/TemplateCommonMethods.cs; 420 RobilityDesigner/ObjectRepository/RespositoryParser.cs; 36, 62 RobilityDesigner/Prompt/ClsPromptJsonManage.cs; 37 RobilityDesigner/Prompt/PromptTree.cs; 66 RobilityDesigner/Prompt/PromptWindow.cs; 139, 148, 171 RobilityDesigner/ReusableObjects/ViewModel/ReusableObjectViewModel.cs; 333, 354 RobilityDesigner/Robility.Launcher/App.xaml.cs; 157 RobilityDesigner/Robility.Launcher/ManageFeatures/ManageFeatureViewModel.cs; 3188, 3385, 3411, 3425, 3758 RobilityDesigner/Robility.Launcher/ViewModel/DesignerLauncherViewModel.cs; 1806, 1860, 4175, 5281 RobilityDesigner/Robility.Launcher/ViewModel/FileUtility.cs; 58, 107 RobilityDesigner/Robility.Launcher/ViewModel/OpenSolution/OpenSolution.cs; 229 RobilityDesigner/Robility.Launcher/ViewModel/OpenSolution/RenameSolution.cs; 252, 259 RobilityDesigner/Robility.Launcher/ViewModel/UpdateFeatures.cs; 438 RobilityDesigner/Robility.Launcher/Views/DesignerLauncher.xaml.cs; 659, 733 RobilityDesigner/Robility.Launcher/Views/NewProject.xaml.cs; 129 RobilityDesigner/Robility.Launcher/Views/Rename.xaml.cs; 91 RobilityDesigner/RobilityRunner/Program.cs; 145 RobilityDesigner/RobilityRunner/WorkflowExecution/Runner.cs; 117, 651 RobilityDesigner/RunnerExecution/RunnerInstanceExecution.cs; 554 RobilityDesigner/RunnerInstance/WorkflowExecution/Runner.cs; 213, 516 RobilityDesigner/TreeViewToolBox/AddTemplateFolder.cs; 119 RobilityDesigner/TreeViewToolBox/TreeviewToolbox.cs; 896, 919 RobilityDesigner/ViewModel/DllImports.cs; 193, 694, 706, 747, 985 RobilityDesigner/ViewModel/Importfiles.cs; 154, 249, 312, 324, 619 RobilityDesigner/ViewModel/InteractActivityFunctions.cs; 236 RobilityDesigner/ViewModel/InvokeTemplateArguments.cs; 57

	RobilityDesigner/ViewModel/MainWindwoActiproViewModel.cs; 1155, 1303, 1824, 3534, 3759, 3770, 4432, 4507, 4689, 5173 RobilityDesigner/ViewModel/RemoveDependencies.cs; 196 RobilityDesigner/ViewModel/RemoveUnusedWorkflows.cs; 153 RobilityDesigner/ViewModel/RenameFolder.cs; 191 RobilityDesigner/ViewModel/SolutionProperties.cs; 123 RobilityDesigner/ViewModel/SolutionPropertiescontextmenus.cs; 1249, 1253, 1260, 1264, 1690, 1729 RobilityDesigner/ViewModel/UpdateDisplyInfo.cs; 26 RobilityDesigner/ViewModel/WorkflowExecution.cs; 849, 900, 1483, 1524, 1580 RobilityDesigner/Views/ProjectProperties.xaml.cs; 59 RobilityDesigner/Views/RenameWorkflow.xaml.cs; 96 RobilityDesigner/Views/SolutionRename.xaml.cs; 102 RobilityDesigner/WorkFlowScan/FolderHasher.cs; 77, 95 RobilityDesigner/WorkFlowScan/LogCleaner.cs; 28 RobilityDesigner/WorkFlowScan/SecurityLogHelper.cs; 176, 221 RobilityDesigner/WorkFlowScan/WorkFlowScanTreeView.cs; 58 RobilityDesigner/WorkflowAnalyzer/SaveReportData.cs; 52, 116 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/package_index.py; 389 Runner/RobilityRunner/Python/Lib/site-packages/PIL/IcnsImagePlugin.py; 391 Runner/RobilityRunner/Python/Lib/site-packages/PIL/Image.py; 2419 Runner/RobilityRunner/Python/Lib/site-packages/PIL/ImageFile.py; 105 Runner/RobilityRunner/Python/Lib/site-packages/PIL/ImageFont.py; 822 Runner/RobilityRunner/Python/Lib/site-packages/PIL/SpiderImagePlugin.py; 83 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/operations/install/wheel.py; 390 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/utils/unpacking.py; 115, 140, 218 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/cachecontrol/caches/file_cache.py; 52 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/distlib/compat.py; 221 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 546 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/pkg_resources/__init__.py; 1896, 1906, 1907, 1929, 3251 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/pygments/formatters/img.py; 128 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/pyproject_hooks/_in_process/_in_process.py; 31, 36 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/rich/console.py; 2275 Runner/RobilityRunner/Python/Lib/site-packages/pkg_resources/__init__.py; 1896, 1906, 1907, 1929, 3251

	Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/config.py; 44 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/file_util.py; 27, 33, 40, 149, 158, 172, 212, 225, 229 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/command/build_ext.py; 298, 341 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/wheel.py; 228, 230 Runner/RobilityRunner/AutoConnectListener.cs; 227 RobilityActivites/ChromeSpy - Copy/AdvanceSpyWindow.xaml.cs; 192 RobilityActivites/ChromeSpy - Copy/MainWindow.xaml.cs; 168 RobilityActivites/ChromeSpy - Copy/View/AdvancedSpyWindow.xaml.cs; 124 RobilityActivites/ChromeSpy - Copy/View/SpyWindow.xaml.cs; 125 RobilityActivites/ChromeSpy/AdvanceSpyWindow.xaml.cs; 201 RobilityActivites/ChromeSpy/MainWindow.xaml.cs; 207 RobilityActivites/ChromeSpy/View/AdvancedSpyWindow.xaml.cs; 124 RobilityActivites/ChromeSpy/View/SpyWindow.xaml.cs; 125 RobilityActivites/GlobalElementEditor/Helper/Connect.cs; 40, 42, 65, 68, 107, 111 RobilityActivites/ImageFunction/ProcessImage.cs; 90, 93, 108, 110, 135 RobilityActivites/JavaElementExtractor/Utils/Settings/UserSettings.cs; 46, 71, 74, 76, 87 RobilityActivites/JavaSpy/Utils/Settings/UserSettings.cs; 46, 71, 74, 76, 87 RobilityActivites/Robility.Cognitive/AbbyyCloudOCR.cs; 278, 377 RobilityActivites/Robility.CoreActivities/Assign.cs; 66, 67, 84 RobilityActivites/Robility.CoreActivities/InvokeVBScript.cs; 77, 79 RobilityActivites/Robility.CoreActivities/KillProcess.cs; 61, 63 RobilityActivites/Robility.CoreActivities/RepeatNumberOfTimes.cs; 96, 97, 126, 244, 245, 250, 251, 252 RobilityActivites/Robility.CoreActivities/StartProcess.cs; 127, 129, 173, 205, 206, 211, 212, 213 RobilityActivites/Robility.DataTable/Common/FilterTableSupportFunctions.cs; 188, 204, 551, 559 RobilityActivites/Robility.DataTable/Common/ValidationCompareData.cs; 25, 30 RobilityActivites/Robility.DataTable/CompareDataTable.cs; 95, 96 RobilityActivites/Robility.DataTable/DatatabletoHTMLfile.cs; 111, 120 RobilityActivites/Robility.DataTable/FilterTable.cs; 83, 84, 101, 122, 123, 138, 141, 155, 169 RobilityActivites/Robility.DataTable/JoinDataTable.cs; 88, 89, 100, 104, 144 RobilityActivites/Robility.DataTable/MergeTable.cs; 81, 82, 86, 90, 123, 128, 145, 146, 150, 151, 160, 166, 170 RobilityActivites/Robility.DataTable/RemoveColumn.cs; 68, 69, 93, 102, 103, 110, 119, 128, 141, 157, 158, 162, 163, 169, 170, 177, 188, 280 RobilityActivites/Robility.DataTable/RemoveDuplicateRow.cs; 58, 59, 65, 76, 79 RobilityActivites/Robility.DataTable/RemoveRow.cs; 64, 65, 94, 100, 106, 110, 116, 123, 129, 142, 143, 146, 147, 161, 162, 172, 173, 179

	RobilityActivites/Robility.DataTable/UpdateRowItem.cs; 87, 88, 124, 129, 134, 140, 150, 168 RobilityActivites/Robility.DesktopAutomationUIA3/ApplicationActions.cs; 122, 158, 172, 202 RobilityActivites/Robility.DesktopAutomationUIA3/ApplicationExist.cs; 106 RobilityActivites/Robility.DesktopAutomationUIA3/BringtoFront.cs; 121, 165, 180, 213 RobilityActivites/Robility.DesktopAutomationUIA3/CheckAppState.cs; 100 RobilityActivites/Robility.DesktopAutomationUIA3/Click.cs; 171, 224, 238, 268 RobilityActivites/Robility.DesktopAutomationUIA3/ExpandCollapse.cs; 197, 249 RobilityActivites/Robility.DesktopAutomationUIA3/FindChildren.cs; 108, 149, 193 RobilityActivites/Robility.DesktopAutomationUIA3/GetAttributeElement.cs; 126, 163, 231 RobilityActivites/Robility.DesktopAutomationUIA3/GetTableData.cs; 103, 143, 222 RobilityActivites/Robility.DesktopAutomationUIA3/GetText.cs; 109, 156, 201 RobilityActivites/Robility.DesktopAutomationUIA3/SecureTypeText.cs; 147, 183, 242 RobilityActivites/Robility.DesktopAutomationUIA3/SelectItem.cs; 123, 170, 214 RobilityActivites/Robility.DesktopAutomationUIA3/SelectList.cs; 90, 130, 174 RobilityActivites/Robility.DesktopAutomationUIA3/TypeText.cs; 143, 188, 232 RobilityActivites/Robility.DesktopAutomationUIA3/Utilities/Common.cs; 51, 67, 68, 90, 96, 120, 149, 155, 156, 184 RobilityActivites/Robility.ExcelAutomation.Tests/BusinessLayer/ChangeDataRangeActivityTests.cs; 63 RobilityActivites/Robility.ExcelAutomation.Tests/BusinessLayer/UpdateAxisBoundsTests.cs; 61 RobilityActivites/Robility.ExcelAutomation.Tests/ChangePivotDataSourceTests.cs; 297 RobilityActivites/Robility.FSAutomation/CopyFile.cs; 131 RobilityActivites/Robility.FSAutomation/CopyFolder.cs; 69, 71, 76, 78, 92, 97, 125, 140, 149, 154, 161, 165, 169, 184, 189, 249, 254, 278, 289 RobilityActivites/Robility.FSAutomation/CreateFile.cs; 214, 249 RobilityActivites/Robility.FSAutomation/FileSystemTrigger.cs; 65, 70, 73, 80 RobilityActivites/Robility.FSAutomation/ForEach.cs; 80, 83, 86, 108, 130, 312, 354, 356, 361, 363 RobilityActivites/Robility.FSAutomation/MoveFile.cs; 248 RobilityActivites/Robility.FSAutomation/Unzip.cs; 64, 67, 87, 93, 108, 111, 113, 116, 128, 132, 137, 141, 153 RobilityActivites/Robility.FormBuilder/Controls/ControlProperties/TextBoxPropertyInfo.cs; 67, 159, 161, 163 RobilityActivites/Robility.FormBuilder/ImageRelatedClass.cs; 57 RobilityActivites/Robility.GoogleSheet/Robility.GoogleSheet/AddSheet.cs; 104, 106, 123

	RobilityActivites/Robility.GoogleSheet/Robility.GoogleSheet/Create.cs; 147, 172, 174 RobilityActivites/Robility.Interact/CheckDuplicateTransaction.cs; 99, 100, 120, 131, 136, 138, 156 RobilityActivites/Robility.JavaApp/CheckAppState.cs; 83, 113 RobilityActivites/Robility.JavaApp/Click.cs; 107, 138, 152, 188 RobilityActivites/Robility.JavaApp/ExpandCollapse.cs; 101, 130, 144, 180 RobilityActivites/Robility.JavaApp/FindChildren.cs; 112, 148, 166, 223 RobilityActivites/Robility.JavaApp/GetAttributeElement.cs; 110, 138, 153, 212 RobilityActivites/Robility.JavaApp/GetTableData.cs; 93, 122, 136, 172 RobilityActivites/Robility.JavaApp/GetText.cs; 97, 126, 140, 176 RobilityActivites/Robility.JavaApp/LaunchJavaApplication.cs; 87, 116, 151 RobilityActivites/Robility.JavaApp/SecureTypeText.cs; 121, 155, 169, 204 RobilityActivites/Robility.JavaApp/SelectItem.cs; 110, 140, 158, 194 RobilityActivites/Robility.JavaApp/TypeText.cs; 118, 149, 164, 199 RobilityActivites/Robility.Json/JsonToDataset.cs; 89, 92, 108, 110, 115, 117, 138, 139, 155, 176 RobilityActivites/Robility.Manager/APIRequest.cs; 311 RobilityActivites/Robility.Manager/Common/Validation.cs; 45, 47, 70, 72, 77, 79 RobilityActivites/Robility.Manager/GetAsset.cs; 128 RobilityActivites/Robility.Manager/GetCredentials.cs; 107, 109, 139, 141, 154, 166, 168, 173, 201, 213, 214, 258, 280 RobilityActivites/Robility.Manager/GetJwtToken.cs; 133 RobilityActivites/Robility.Manager/GetPinandKey.cs; 140 RobilityActivites/Robility.Manager/GetToken.cs; 133 RobilityActivites/Robility.Manager/SetAsset.cs; 116 RobilityActivites/Robility.MicrosoftOutlook365/SetEmailCategories.cs; 121, 125 RobilityActivites/Robility.OSFunctionsAutomation/AppendLine.cs; 110 RobilityActivites/Robility.OSFunctionsAutomation/ReadText.cs; 97 RobilityActivites/Robility.OSFunctionsAutomation/WriteText.cs; 114 RobilityActivites/Robility.OutlookAutomation/CopyFolder.cs; 77, 81, 152, 159, 216, 221, 231, 239, 251, 253, 258, 260 RobilityActivites/Robility.OutlookAutomation/EmailTrigger.cs; 71, 78, 81, 92, 218, 223 RobilityActivites/Robility.OutlookAutomation/ForEachMail.cs; 110, 115, 118, 123 RobilityActivites/Robility.OutlookAutomation/Forward.cs; 91, 94, 105, 117, 121, 129, 134, 151, 208, 214, 219, 221, 236, 238, 243 RobilityActivites/Robility.OutlookAutomation/MarkAsReadUnread.cs; 53, 58, 61, 66, 105, 107, 118, 123 RobilityActivites/Robility.OutlookAutomation/Move.cs; 76, 79, 94, 101, 106, 109, 144, 146, 151, 153 RobilityActivites/Robility.OutlookAutomation/NewMail.cs; 89, 92, 148, 164, 167, 172, 181, 187, 192, 194, 217, 219, 224, 226

	RobilityActivites/Robility.OutlookAutomation/OutlookScope.cs; 57, 63, 66, 73, 80, 94, 99, 113, 132, 142, 144, 149, 151 RobilityActivites/Robility.OutlookAutomation/Reply.cs; 96, 99, 133, 136, 170, 172, 192, 200, 218, 226, 240, 246, 251, 253, 268, 270, 275 RobilityActivites/Robility.OutlookAutomation/Save.cs; 67, 70, 80, 82, 92, 107, 130, 145, 157, 171, 173, 178, 180 RobilityActivites/Robility.PDFAutomation/ClsUtilities.cs; 108 RobilityActivites/Robility.PDFAutomation/ConverToPDF.cs; 92, 95, 136 RobilityActivites/Robility.PDFAutomation/ExtractImagesFromPdf.cs; 89, 104, 107 RobilityActivites/Robility.PDFAutomation/MergeFiles.cs; 79, 90, 94, 122, 134, 136, 142, 145 RobilityActivites/Robility.PDFAutomation/MergePages.cs; 72, 79, 82, 88, 97, 101, 107, 128, 130, 135, 223, 231, 239, 247 RobilityActivites/Robility.PDFAutomation/PdfCreate.cs; 92, 104, 108, 153, 162 RobilityActivites/Robility.PDFAutomation/PdfPageToImage.cs; 72, 84, 88, 144, 148, 154, 157, 180, 187, 190, 197, 200 RobilityActivites/Robility.PDFAutomation/PdfPagecount.cs; 59, 66, 69, 109, 111, 116, 118 RobilityActivites/Robility.PDFAutomation/Split.cs; 82, 89, 91, 146, 147, 192, 194, 199, 201 RobilityActivites/Robility.PDFAutomation/TextExtractor.cs; 67, 75, 79, 114, 116, 121, 123 RobilityActivites/Robility.SQliteAutomation/CreateTable.cs; 367 RobilityActivites/Robility.SQliteAutomation/DBBackup.cs; 284, 285, 297, 298, 319, 320, 332, 333 RobilityActivites/Robility.SQliteAutomation/DropTable.cs; 241, 248, 249, 298, 299, 310, 311 RobilityActivites/Robility.SQliteAutomation/EncryptDecrypt.cs; 31, 39, 98, 109, 121, 129 RobilityActivites/Robility.SQliteAutomation/ExecuteNonQuery.cs; 261, 268, 269, 327, 328, 339, 340 RobilityActivites/Robility.SQliteAutomation/ExecuteQuery.cs; 157, 158, 169, 170 RobilityActivites/Robility.SQliteAutomation/ExportCSV.cs; 329, 330, 341, 342, 363, 372, 373 RobilityActivites/Robility.SQliteAutomation/ImportData.cs; 219, 220, 230, 231 RobilityActivites/Robility.SmartRPACognitiveServices/spacyNLTK.py; 8 RobilityActivites/Robility.TextAutomation/AppendText.cs; 76, 81, 145, 177, 178, 182, 183, 192, 194 RobilityActivites/Robility.TextAutomation/Clsutility.cs; 102 RobilityActivites/Robility.TextAutomation/OverWriteText.cs; 90, 93, 102, 109, 111, 133, 134, 138, 139 RobilityActivites/Robility.TextAutomation/ReadText.cs; 102, 105, 116, 122, 134, 135, 139, 140

	RobilityActivites/Robility.TextAutomation/TableParserCSV.cs; 73, 76, 81, 112, 121, 156, 203, 207, 211, 215, 226, 227, 231, 232 RobilityActivites/Robility.TextAutomation/TextSplitting.cs; 74, 78, 84, 97, 103, 118, 120, 125, 127, 141 RobilityActivites/Robility.WebAutomation_V3/ExtractData.cs; 325, 360, 361 RobilityActivites/Robility.WordDocument/ReadText.cs; 87, 89, 110, 137 RobilityActivites/Robility.WordDocument/SaveWordAsPDF.cs; 70, 72 RobilityActivites/RobilityWebClient/Soap.cs; 236, 239, 281, 283 RobilityActivites/SpyCommunicator/WebSpyCommunication/FileWatcherCls.cs; 97 RobilityActivites/UIExplore/PluginsHandlers/BrowserSpyCommunicator.cs; 62 RobilityActivites/UIExplore/UIExplore/PluginsHandlers/BrowserSpyCommunicator.cs; 60 RobilityActivites/WebCommunicator/FileWatcher/FileWatcherCls.cs; 84 RobilityActivites/GlobalElementEditor/Helper/Connect.cs; 63 RobilityActivites/JavaElementExtractor/Utils/Settings/UserSettings.cs; 41, 72, 85 RobilityActivites/JavaSpy/Utils/Settings/UserSettings.cs; 41, 72, 85 RobilityActivites/ModernDesktopExecutorLib/Utilities/LaunchUwpApps.cs; 65 RobilityActivites/Robility.Cognitive/AbbyyCloudOCR.cs; 269, 376 RobilityActivites/Robility.CoreActivities/StartProcessHelper .cs; 270 RobilityActivites/Robility.DataTable/DatatabletoHTMLfile.cs; 105 RobilityActivites/Robility.DesktopAutomation/Utilities/LaunchUwpApps.cs; 65 RobilityActivites/Robility.ExcelAutomation.Tests/BusinessLayer/ChangeDataRangeActivityTests.cs; 61 RobilityActivites/Robility.ExcelAutomation.Tests/BusinessLayer/UpdateAxisBoundsTests.cs; 59 RobilityActivites/Robility.ExcelAutomation.Tests/ChangePivotDataSourceTests.cs; 295 RobilityActivites/Robility.FSAutomation/CopyFile.cs; 129 RobilityActivites/Robility.FSAutomation/CreateFile.cs; 195, 197, 212, 230, 232, 245, 248, 271, 316 RobilityActivites/Robility.FSAutomation/MoveFile.cs; 215, 246 RobilityActivites/Robility.FormBuilder/Designer/CustomForm.xaml.cs; 1287, 9773, 10001, 10083 RobilityActivites/Robility.Invoke/InvokeDll.cs; 91 RobilityActivites/Robility.MailAutomation.Outlook/ClsForward.cs; 24 RobilityActivites/Robility.MailAutomation.Outlook/ClsSend.cs; 56 RobilityActivites/Robility.MailAutomation.Outlook/Reply.cs; 212 RobilityActivites/Robility.OSFunctionsAutomation/AppendLine.cs; 150 RobilityActivites/Robility.OSFunctionsAutomation/ReadText.cs; 95 RobilityActivites/Robility.OSFunctionsAutomation/WriteText.cs; 132 RobilityActivites/Robility.OutlookAutomation/Save.cs; 120 RobilityActivites/Robility.SQliteAutomation/CreateTable.cs; 365 RobilityActivites/Robility.SQliteAutomation/DBBackup.cs; 182, 287, 322 RobilityActivites/Robility.SQliteAutomation/DropTable.cs; 192, 235, 239, 296, 301

	RobilityActivites/Robility.SQliteAutomation/EncryptDecrypt.cs; 95, 107 RobilityActivites/Robility.SQliteAutomation/ExecuteNonQuery.cs; 196, 259, 325, 330 RobilityActivites/Robility.SQliteAutomation/ExecuteQuery.cs; 155, 160, 215 RobilityActivites/Robility.SQliteAutomation/ExportCSV.cs; 211, 327, 332, 359, 361 RobilityActivites/Robility.SQliteAutomation/ImportData.cs; 217, 222, 311 RobilityActivites/Robility.TextAutomation/Clsutility.cs; 136, 203
Observation	During assessment it was observed that the attackers can control the file system path argument, which allows them to access or modify otherwise protected files.
Severity Rating	**Medium**
Impact	Path manipulation errors occur when the following two conditions are met: • An attacker can specify a path used in an operation on the file system. • By specifying the resource, the attacker gains a capability that would not otherwise be permitted.
Recommendation	It is recommended to create a list of legitimate values from which the user must select. With this approach, the user-provided input is never used directly to specify the resource name.
References	https://vulncat.fortify.com/en/detail?category=Path+Manipulation

Proof of Concept:

package_index.py

```
386
387         if os.path.isdir(fn) and not nested:
388             path = os.path.realpath(fn)
389             for item in os.listdir(path):
390                 self.process_filename(os.path.join(path, item), True)
```

FIGURE 7: PATH MANIPULATION

8. PRIVACY VIOLATION

Source File	RobilityDesigner/Python/Lib/site-packages/pip/_vendor/rich/prompt.py; 370 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/config.py; 45 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/rich/prompt.py; 370 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/config.py; 45 RobilityActivites/Robility.PDFAutomation/PdfPageToImage.cs; 161 RobilityActivites/Robility.PDFAutomation/PdfPagecount.cs; 120 RobilityActivites/Robility.PDFAutomation/Split.cs; 203 RobilityActivites/Robility.PDFAutomation/TextExtractor.cs; 125 RobilityActivites/Robility.FSAutomation/Zip.cs; 202
Observation	During assessment it was observed that the mentioned method mishandles confidential information, which can compromise user privacy and is often illegal.
Severity Rating	**Medium**
Impact	Privacy violations occur when: • Private user information enters the program. • The data is written to an external location, such as the console, file system or network.
Recommendation	It is recommended that when security and privacy demands clash, privacy should usually be given the higher priority. To accomplish this and still maintain required security information, cleanse any private information before it exits the program.
References	https://www.theregister.co.uk/2005/02/07/aol_email_theft/

Proof of Concept:

config.py

```
42          """Creates a default .pypirc file."""
43          rc = self._get_rc_file()
44          with os.fdopen(os.open(rc, os.O_CREAT | os.O_WRONLY, 0o600), 'w') as f:
45              f.write(DEFAULT_PYPIRC % (username, password))
```

FIGURE 8: PRIVACY VIOLATION

9. WEAK ENCRYPTION

Source File	RobilityActivites/Robility.CryptographyAutomation/Utility.cs; 149, 151, 155
Observation	During assessment it was observed that the mentioned call uses a cryptographic encryption algorithm that cannot guarantee the confidentiality of sensitive data.
Severity Rating	**Medium**
Impact	Antiquated encryption algorithms such as DES no longer provide sufficient protection for use with sensitive data. Encryption algorithms rely on key size as one of the primary mechanisms to ensure cryptographic strength. Cryptographic strength is often measured by the time and computational power needed to generate a valid key.
Recommendation	Use strong encryption algorithms with large key sizes to protect sensitive data. A strong alternative to DES is AES (Advanced Encryption Standard, formerly Rijndael). Before selecting an algorithm, first determine if your organization has standardized on a specific algorithm and implementation.
References	http://www.distributed.net/des/

Proof of Concept:

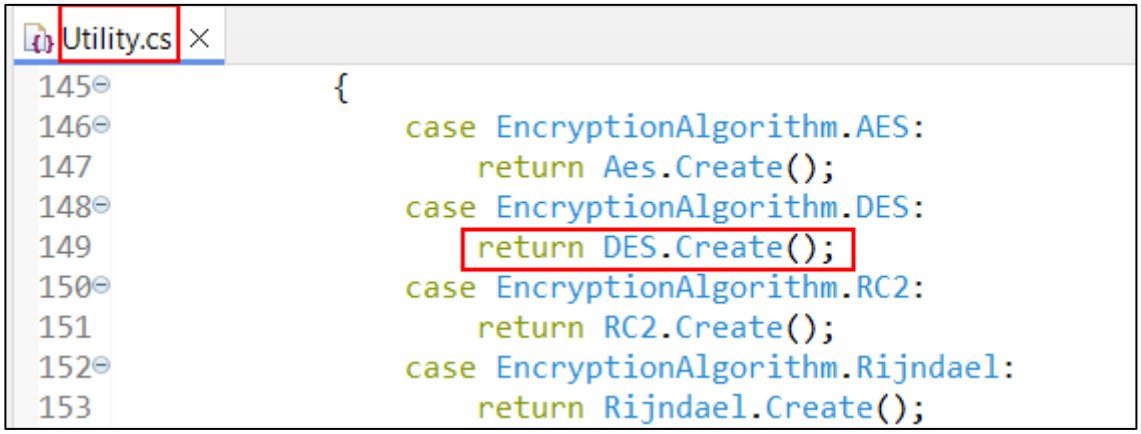


FIGURE 9: WEAK ENCRYPTION

10. ASP.NET MVC BAD PRACTICES: MODEL WITH REQUIRED NON-NULLABLE PROPERTY	
Source File	RobilityActivites/Robility.UIVision/Highlight.cs; 40
Observation	During assessment it was observed that the model class Highlight has a required non-nullable property and therefore may be susceptible to under-posting attacks.
Severity Rating	Medium
Impact	Using a model class that has non-nullable properties that are required (as marked with the [Required] attribute) can lead to problems if an attacker communicates a request that contains less data than is expected.
Recommendation	It is recommended to: • Wrap non-nullable types in a Nullable. If an attacker does not communicate a value, then the property will be null and will not satisfy the [Required] validation attribute. • Define the default value of zero as a safe default or as a known invalid value.
References	http://bradwilson.typepad.com/blog/2010/01/input-validation-vs-model-validation-in-aspnet-mvc.html

Proof of Concept:

Highlight.cs

```
36          [Category("Input")]
37          [DisplayName("Highlight Color")]
38          [Required]
39          [Description("Specify the color of the highlight")]
40          public HighlightColor SelectedHighlightColor { get; set; }
41
```

FIGURE 10: ASP.NET MVC BAD PRACTICES: MODEL WITH REQUIRED NON-NULLABLE PROPERTY

11. CROSS-SITE SCRIPTING: REFLECTED	
Source File	RobilityWebClient/clsFunction.cs; 355
Observation	During assessment it was observed that the mentioned method sends unvalidated data to a web browse, which can result in the browser executing malicious code.
Severity Rating	**Medium**
Impact	Cross-site scripting (XSS) vulnerabilities occur when: • Data enters a web application through an untrusted source. In the case of reflected XSS, the untrusted source is typically a web request, while in the case of persisted (also known as stored) XSS it is typically a database or other back-end data store. • The data is included in dynamic content that is sent to a web user without validation.
Recommendation	It is recommended to ensure that validation occurs in the required places and that relevant properties are set to prevent vulnerabilities.
References	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496719#9

Proof of Concept:

clsFunction.cs

```
353                 using (Stream stm = httpWebRequest.GetRequestStream())
354                 {
355                     stm.Write(buffer, 0, buffer.Length);
356                 }
```

FIGURE 11: CROSS-SITE SCRIPTING: REFLECTED

12. DYNAMIC CODE EVALUATION: CODE INJECTION	
Source File	RobilityDesigner/Python/Lib/site-packages/pip/_vendor/pkg_resources/__init__.py; 1561 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/pygments/formatters/__init__.py; 103 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/pygments/lexers/__init__.py; 153 RobilityDesigner/Python/Lib/site-packages/pkg_resources/__init__.py; 1561 RobilityDesigner/Python/Lib/site-packages/setuptools/sandbox.py; 46 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/pkg_resources/__init__.py; 1561 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/pygments/formatters/__init__.py; 103 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/pygments/lexers/__init__.py; 153 Runner/RobilityRunner/Python/Lib/site-packages/pkg_resources/__init__.py; 1561 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/sandbox.py; 46
Observation	During assessment it was observed that the file interprets unvalidated user input as source code. Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code.
Severity Rating	Medium
Impact	Many modern programming languages allow dynamic interpretation of source instructions. This capability allows programmers to perform dynamic instructions based on input received from the user. Code injection vulnerabilities occur when the programmer incorrectly assumes that instructions supplied directly from the user will perform only innocent operations, such as performing simple calculations on active user objects or otherwise modifying the user's state. However, without proper validation, a user might specify operations the programmer does not intend.
Recommendation	It is recommended to avoid dynamic code interpretation whenever possible.
References	https://vulncat.fortify.com/en/detail?category=Dynamic+Code+Evaluation&subcategory=Code+Injection

Proof of Concept:

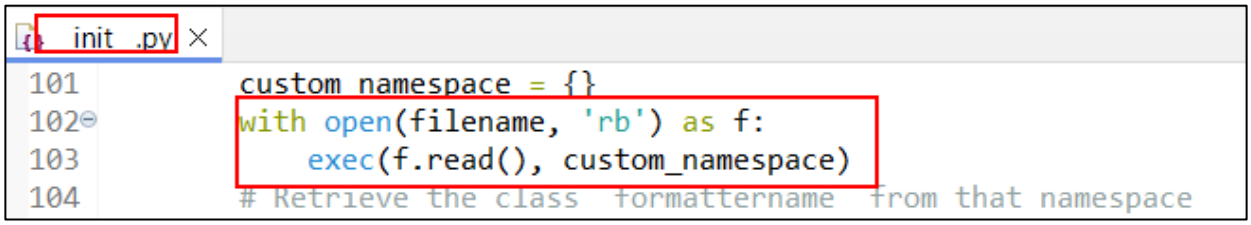


FIGURE 12: DYNAMIC CODE EVALUATION: CODE INJECTION

13. INSECURE RANDOMNESS	
Source File	RobilityDesigner/Python/Lib/site-packages/PIL/ImagePalette.py; 230 RobilityDesigner/Python/Lib/site-packages/pip/_internal/utils/filesystem.py; 100 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/rich/live.py; 352, 355 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/rich/progress.py; 1701 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/rich/style.py; 193, 243, 490, 642, 688 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/tenacity/wait.py; 72, 194, 222 RobilityDesigner/Python/Lib/site-packages/pkg_resources/_vendor/more_itertools/more.py; 3465, 3469, 3473, 3475, 3476, 3486, 3496, 3504, 3508 RobilityDesigner/Python/Lib/site-packages/pkg_resources/_vendor/more_itertools/recipes.py; 592, 642 RobilityDesigner/Python/Lib/site-packages/setuptools/_vendor/more_itertools/more.py; 3288, 3292, 3297, 3299, 3300, 3310, 3320, 3328, 3332 RobilityDesigner/Python/Lib/site-packages/setuptools/_vendor/more_itertools/recipes.py; 492, 542 RobilityDesigner/Python/Lib/site-packages/setuptools/command/easy_install.py; 442 RobilityDesigner/RobilityRunner/Utilities/SocketPort.cs; 39 Runner/RobilityRunner/Python/Lib/site-packages/PIL/ImagePalette.py; 230 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/utils/filesystem.py; 100 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/rich/live.py; 352, 355 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/rich/progress.py; 1701 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/rich/style.py; 193, 243, 490, 642, 688 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/tenacity/wait.py; 72, 194, 222 Runner/RobilityRunner/Python/Lib/site-packages/pkg_resources/_vendor/more_itertools/more.py; 3465, 3469, 3473, 3475, 3476, 3486, 3496, 3504, 3508 Runner/RobilityRunner/Python/Lib/site-packages/pkg_resources/_vendor/more_itertools/recipes.py; 592, 642 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_vendor/more_itertools/more.py; 3288, 3292, 3297, 3299, 3300, 3310, 3320, 3328, 3332 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_vendor/more_itertools/recipes.py; 492, 542

	Runner/RobilityRunner/Python/Lib/site-packages/setuptools/command/easy_install.py; 442
Observation	During assessment it was observed that the random number generator implemented by random() cannot withstand a cryptographic attack.
Severity Rating	**Medium**
Impact	Insecure randomness errors occur when a function that can produce predictable values is used as a source of randomness in a security-sensitive context.
Recommendation	It is recommended that when unpredictability is critical, as is the case with most security-sensitive uses of randomness, use a cryptographic PRNG.
References	https://vulncat.fortify.com/en/detail?category=Insecure+Randomness

Proof of Concept:

easy_install.py

```
440             pid = os.getpid()
441         except Exception:
442             pid = random.randint(0, sys.maxsize)
443         return os.path.join(self.install_dir, "test-easy-install-%s" % pid)
```

FIGURE 13: INSECURE RANDOMNESS

14. KEY MANAGEMENT: HARDCODED PBE PASSWORD	
Source File	SmartRPALogonService/Service References/WebService/Reference.cs; 237 SmartRPALogonService/Service References/LogonService/Reference.cs; 391 Robility.ExcelAutomation/Common/EncryptionService.cs; 42 WorkflowServices/Service References/WorkflowServiceClient/Reference.cs; 1911 WorkflowServices_Live/Service References/WorkflowServiceClient/Reference.cs; 1911
Observation	During assessment it was observed that a hardcoded password is used to generate a key from a password-based key derivation function (PBKDF). Providing a hardcoded password to a PBKDF compromises system security in a way that is not easily remedied.
Severity Rating	**Medium**
Impact	It is never a good idea to pass an empty value as the password argument to a cryptographic password-based key derivation function (PBKDF).
Recommendation	It is recommended to never use password-based key derivation functions to generate a cryptographic key based on a hardcoded password.
References	https://vulncat.fortify.com/en/detail?category=Key+Management&subcategory=Hardcoded+PBE+Password

Proof of Concept:

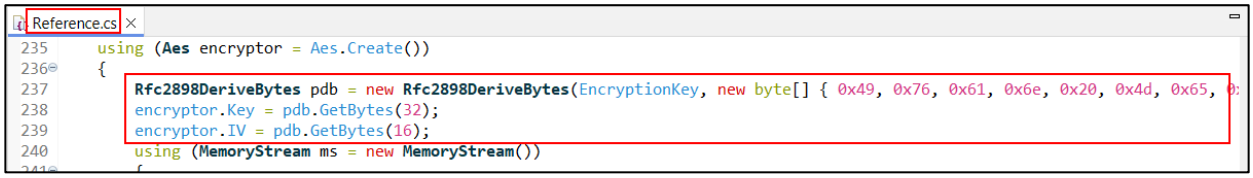


FIGURE 14: KEY MANAGEMENT: HARDCODED PBE PASSWORD

15. PASSWORD MANAGEMENT: EMPTY PASSWORD	
Source File	RobilityDesigner/Functions/GitLeaksScannerLib/GitLeaksScanner.cs; 397 RobilityDesigner/Functions/SmartRPAActivities/GlobalVariables.cs; 221 RobilityDesigner/Python/Lib/site-packages/pip/_internal/utils/misc.py; 474 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/command/register.py; 143 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/command/upload.py; 42 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/dist.py; 208 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/utils/misc.py; 474 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/command/register.py; 143 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/command/upload.py; 42 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/dist.py; 208 RobilityActivites/Robility.DesktopAutomation/SecureTypeText.cs; 435 RobilityActivites/Robility.InternetExplorer/SecureSetText.cs; 517 RobilityActivites/Robility.WebAutomation/SecureSetText.cs; 2199
Observation	During assessment it was observed that an empty string is used as a password which is insecure.
Severity Rating	Medium
Impact	It is never appropriate to use an empty string as a password. It is too easy to guess.
Recommendation	It is recommended to use sufficiently hard-to-guess passwords protect all accounts and system resources. Consult the references to help establish appropriate password guidelines.
References	https://vulncat.fortify.com/en/detail?category=Password+Management&subcategory=Empty+Password
Proof of Concept:	

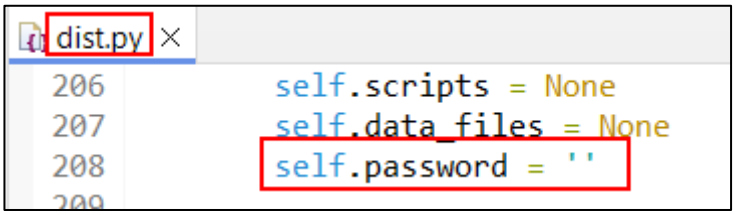


FIGURE 15: PASSWORD MANAGEMENT: EMPTY PASSWORD

16. PASSWORD MANAGEMENT: HARDCODED PASSWORD	
Source File	RobilityDesigner/Pipeline/SonarQube/RobilityDesigner-App-SQ-Dev.yml; 74 Runner/Pipeline/Staging/Runner7App-Pipeline.yml; 205 RobilityActivites/Pipeline/SonarQube/RobilityInteract-SQ_Staging.yml; 79 RobilityActivites/Pipeline/SonarQube/RobilityWebClient-SQ.yml; 67 RobilityActivites/Pipeline/SonarQube/RobilityWordDocument-SQ.yml; 67 RobilityActivites/Pipeline/SonarQube/Robility_ActiveDirectory-SQ.yml; 63 RobilityActivites/Pipeline/SonarQube/Robility_AmazonRekognition-SQ.yml; 63 RobilityActivites/Pipeline/SonarQube/Robility_AmazonS3-SQ.yml; 63 RobilityActivites/Pipeline/SonarQube/Robility_AssistedVirtualSession-SQ.yml; 63 RobilityActivites/Pipeline/SonarQube/Robility_AylienEntityExtraction-SQ.yml; 63 RobilityActivites/Pipeline/SonarQube/Robility_AzureAIFormRecognizer-SQ.yml; 63 RobilityActivites/Robility.ExcelAutomation.Tests/BusinessLayer/SaveExcelBusinessLogicTests.cs; 133 RobilityActivites/Robility.PDFAutomation.Tests/BusinessLayer/FileConvertionsTests.cs; 78, 112 RobilityActivites/Robility.PDFAutomation.Tests/BusinessLayer/PdfPageToImageTest.cs; 54, 128 RobilityActivites/Robility.PDFAutomation.Tests/BusinessLayer/PdfPagecounterTest.cs; 69, 140 RobilityActivites/Robility.PDFAutomation.Tests/BusinessLayer/SplitTest.cs; 51, 66, 175, 192 RobilityActivites/Robility.PDFAutomation.Tests/BusinessLayer/TextExtractorTest.cs; 67, 141 RobilityActivites/Robility.Terminal/TerminalClass/Constants.cs; 19
Observation	During assessment it was observed that hardcoded passwords can compromise system security in a way that is not easy to remedy.
Severity Rating	**Medium**
Impact	It is never a good idea to hardcode a password. Not only does hardcoding a password allow all of the project's developers to view the password, it also makes fixing the problem extremely difficult. After the code is in production, the password cannot be changed without patching the software. If the account protected by the password is compromised, the owners of the system must choose between security and availability.
Recommendation	It is recommended that passwords should never be hardcoded and should generally be obfuscated and managed in an external source. Storing passwords in plain text anywhere on the system allows anyone with sufficient permissions to read and potentially misuse the password.
References	https://docs.microsoft.com/en-us/aspnet/web-forms/overview/data-access/advanced-data-access-scenarios/protecting-connection-strings-and-other-configuration-information-cs
Proof of Concept:	

Runner7App-Pipeline.yml

```
203                 SmtpPort: '25'
204                 SmtpUsername: 'marimuthu.m@sutherlandglobal.com'
205                 SmtpPassword: '!!Nov060792'
206                 UseSSL: false
```

FIGURE 16: PASSWORD MANAGEMENT: HARDCODED PASSWORD

17. PRIVACY VIOLATION: HEAP INSPECTION	
Source File	RobilityDesigner/Functions/ExpressionEditorService/Instance.cs; 228 RobilityDesigner/Functions/SmartRPAActivities/GlobalVariables.cs; 505, 584 RobilityDesigner/Functions/SmartRPAActivities/RobotFunctions.cs; 1052, 1059, 1105, 1112, 1302 RobilityDesigner/Functions/SmartRPAActivities/TemplateCommonMethods.cs; 127 RobilityDesigner/Robility.Launcher/AppSupportClasses/AppCommonMethods.cs; 64 RobilityDesigner/Robility.Launcher/ViewModel/ConnectFormViewModel.cs; 959 RobilityDesigner/Robility.Launcher/ViewModel/DownloadUpgradePackage.cs; 234 RobilityDesigner/Robility.Launcher/ViewModel/FileUtility.cs; 163 RobilityDesigner/RunnerExecution/RunnerInstanceExecution.cs; 602, 1545 RobilityDesigner/SaveWorkflowDetails.cs; 52 RobilityDesigner/ViewModel/PublishSolutionToManager.cs; 107 RobilityDesigner/ViewModel/SupportPublish/PublishObjectHelper.cs; 113 RobilityDesigner/ViewModel/WorkflowViewModel.cs; 1406, 1434 RobilityDesigner/WorkFlowScan/FolderHasher.cs; 116 RobilityDesigner/WorkFlowScan/SecurityLogHelper.cs; 98 RobilityDesigner/WorkflowServices/WorkflowServices.cs; 1009, 1016, 1073, 1080, 1119 RobilityDesigner/WorkflowServices_Live/WorkflowServices.cs; 1019, 1026, 1083, 1090, 1129 Runner/CommonHelper/Helper.cs; 236, 289, 333 Runner/SmartRPALogonService/LogonClass/AutoLogon.cs; 60, 61, 85, 92, 102 Runner/SmartRPALogonService/LogonClass/DecryptAes.cs; 37, 69 RobilityActivites/ImageFunction_6/ClsSearch_Image.cs; 99, 150, 188, 234 RobilityActivites/JavaElementExtractor/Utils/Settings/UserSettings.cs; 40, 69, 70, 84, 217 RobilityActivites/JavaSpy/Utils/Settings/UserSettings.cs; 40, 69, 70, 84, 217 RobilityActivites/Robility.CryptographyAutomation/FileUtility.cs; 72 RobilityActivites/Robility.DBAutomation/ConnectDB.cs; 109, 183 RobilityActivites/Robility.DBAutomation/DSN.cs; 143, 146 RobilityActivites/Robility.DesktopAutomation/Automation/UIAutomation/GetAttributesandPattern.cs; 57, 61, 65, 66, 69, 71, 75, 77, 79, 82 RobilityActivites/Robility.DesktopAutomation/SecureSetText.cs; 227 RobilityActivites/Robility.DesktopAutomation/SecureTypeText.cs; 235, 536 RobilityActivites/Robility.DesktopAutomationUIA3/SecureTypeText.cs; 256 RobilityActivites/Robility.DesktopAutomation_Production/Automation/UIAutomation/GetAttributesandPattern.cs; 51, 55, 59, 60, 63, 65, 69, 71, 73, 76 RobilityActivites/Robility.ExcelAutomation/ExcelScopeUtility.cs; 116 RobilityActivites/Robility.FTPAutomation/CreateDirectory.cs; 70 RobilityActivites/Robility.FTPAutomation/DirectoryExists.cs; 73 RobilityActivites/Robility.FTPAutomation/Download.cs; 83

	RobilityActivites/Robility.FTPAutomation/FileExists.cs; 66 RobilityActivites/Robility.FTPAutomation/RemoveDirectory.cs; 64 RobilityActivites/Robility.FTPAutomation/RemoveFile.cs; 60 RobilityActivites/Robility.FTPAutomation/Upload.cs; 69 RobilityActivites/Robility.FormBuilder/Designer/RunTimeSupportingClass.cs; 163, 164, 234, 235 RobilityActivites/Robility.FormBuilder/Designer/TabItemInfo.xaml.cs; 476 RobilityActivites/Robility.ImageAutomation/ClsImageExists.cs; 56 RobilityActivites/Robility.ImageAutomation/ClsSearch_Image.cs; 166, 197, 268 RobilityActivites/Robility.JavaApp/SecureTypeText.cs; 217 RobilityActivites/Robility.ModernDesktopAutomation/SecureTypeText.cs; 164 RobilityActivites/Robility.PDFAutomation/ClsUtilities.cs; 151 RobilityActivites/Robility.PDFAutomation/PdfPageToImage.cs; 138 RobilityActivites/Robility.PDFAutomation/PdfPagecount.cs; 105 RobilityActivites/Robility.PDFAutomation/Split.cs; 188 RobilityActivites/Robility.PDFAutomation/TextExtractor.cs; 110 RobilityActivites/Robility.ScreenRecording/CompressVideo.cs; 22, 35, 36 RobilityActivites/Robility.ServiceNow/RestService.cs; 53 RobilityActivites/Robility.SmartInteract/Common.cs; 87 RobilityActivites/Robility.Terminal/Common/SecureClass.cs; 55 RobilityActivites/Robility.WebAutomation/SecureSetText.cs; 400, 445, 490, 535, 578, 631, 666, 700, 733, 765, 817, 825, 827, 876, 884, 886, 933, 942, 944, 991, 999, 1001, 1046, 1054, 1056, 1294, 1339, 1384, 1429, 1472, 1525, 1560, 1594, 1627, 1659, 1711, 1719, 1721, 1770, 1778, 1780, 1827, 1836, 1838, 1885, 1893, 1895, 1940, 1948, 1950, 2010, 2036, 2060, 2085, 2111, 2303, 2305, 2341, 2353, 2380, 2382, 2580 RobilityActivites/Robility.WebAutomation_V3/SecureSetText.cs; 584 RobilityActivites/RobilityVideoRecorder/CompressVideo.cs; 22, 35, 36 RobilityActivites/RobilityWebClient/Designer/DesignerRestPartial.cs; 29, 35 RobilityActivites/RobilityWebClient/RestConsumer.cs; 124 RobilityActivites/RobilityWebClient/clsFunction.cs; 335, 694 RobilityActivites/UIExplore/DesktopSpy/TreeNode.cs; 31, 35, 39, 40, 43, 45 RobilityActivites/UIExplore/UIExplore/DesktopSpy/TreeNode.cs; 28, 32, 36, 37, 40, 42 RobilityActivites/UIExplore/UIExplore/Views/MainWindow.xaml.cs; 1876, 1909, 2023, 2027, 2031, 2032, 2035, 2037 RobilityActivites/UIExplore/Views/MainWindow.xaml.cs; 382, 1123, 1148, 1246, 1250, 1254, 1255, 1258, 1260
Observation	During assessment it was observed that the mentioned method stores sensitive data in an insecure manner, making it possible to extract the data via inspecting the heap.
Severity Rating	**Medium**
Impact	Sensitive data (such as passwords, social security numbers, credit card numbers etc.) stored in memory can be leaked if it is stored in a managed String object.

	String objects are not pinned, so the garbage collector can relocate these objects at will and leave several copies in memory.
Recommendation	It is recommended that instead of storing sensitive data in objects such as Strings, store them in an array, which can be nullified and/or encrypted in memory.
References	http://msdn.microsoft.com/en-us/library/atxe881w.aspx

Proof of Concept:

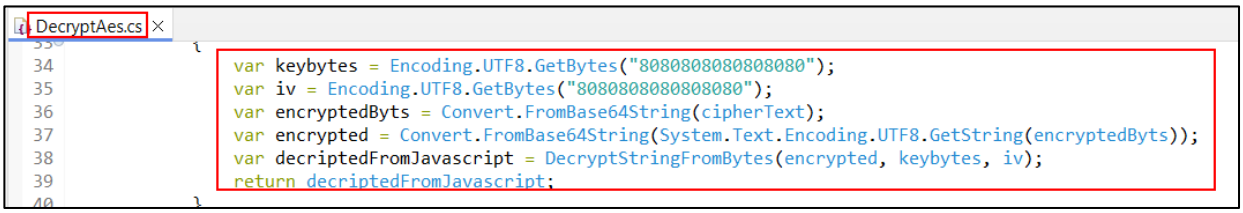


FIGURE 17: PRIVACY VIOLATION: HEAP INSPECTION

18. PROCESS CONTROL	
Source File	RobilityDesigner/ChildSessionRunnerInstance/WorkflowExecution/Runner.cs; 180 RobilityDesigner/DllManagement/DynamicDllManagement.cs; 88 RobilityDesigner/Functions/ExecuteXamlWorkflow/BindDllMethods.cs; 62, 89, 184, 223, 244 RobilityDesigner/Functions/ExecuteXamlWorkflow/InvokeDll.cs; 475 RobilityDesigner/RobilityRunner/WorkflowExecution/Runner.cs; 199 RobilityDesigner/RunnerInstance/WorkflowExecution/Runner.cs; 342 RobilityDesigner/ViewModel/DllImports.cs; 526 RobilityDesigner/ViewModel/WorkflowExecution.cs; 861 Runner/RunnerInstance/WorkflowExecution/FeatureAssembly.cs; 156 RobilityActivites/Robility.CoreActivities/CodeEditor.cs; 128 RobilityActivites/Robility.CoreActivities/CodeEditorVB.cs; 48 RobilityActivites/Robility.CoreActivities/SyntaxEditorHelper.cs; 76 RobilityActivites/Robility.Invoke/BindDllMethods.cs; 66, 169, 187
Observation	During assessment it was observed that the mentioned method is loading a library or executable from an untrusted source or in an untrusted environment. This call can cause an application to execute malicious code on behalf of an attacker.
Severity Rating	Medium
Impact	Process control vulnerabilities take two forms: - An attacker can change the name of the library or executable that the program loads: the attacker explicitly controls what the name of the library or executable is. - An attacker can change the environment in which the library or executable loads: the attacker implicitly controls what the library or executable name means.
Recommendation	It is recommended to not allow users to control libraries or executables loaded by the program. In cases where user input must affect the choice of the library or executable to load, the application typically expects a particular input to take on only a very small set of values.
References	https://msdn.microsoft.com/en-us/library/system.appdomain.executeassembly(v=vs.110).aspx

Proof of Concept:

FeatureAssembly.cs

```
153         private static void LoadAssemeblyCurrentDomain(string assemblyPath, string path)
154         {
155             AppDomain.CurrentDomain.AppendPrivatePath(path);
156             Assembly assembly = Assembly.LoadFrom(assemblyPath);
157             AppDomain.CurrentDomain.Load(assembly.GetName());
158         }
```

FIGURE 18: PROCESS CONTROL

19. SERVER-SIDE REQUEST FORGERY	
Source File	RobilityDesigner/Functions/SmartSpy/MainWindow.xaml.cs; 134 RobilityDesigner/Python/Lib/site-packages/setuptools/package_index.py; 1072, 1109 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/package_index.py; 1072, 1109 RobilityActivites/Robility.FTPAutomation/clsFTP.cs; 194, 215, 238, 251 RobilityActivites/Robility.FormBuilder/Controls/UpdateControls/UpdateLabelControl.cs; 34 RobilityActivites/Robility.FormBuilder/Designer/CustomForm.xaml.cs; 1475 RobilityActivites/Robility.GoogleSheet/Robility.GoogleSheet/AddSheet.cs; 170 RobilityActivites/Robility.MicrosoftComputerVision/ExtractHandwrittenText.cs; 265 RobilityActivites/RobilityWebClient/clsFunction.cs; 299 RobilityActivites/Robility.ServiceNow/RestService.cs; 65, 68, 72, 76 RobilityActivites/RobilityWebClient/clsFunction.cs; 569
Observation	During assessment it was observed that the mentioned function initiates a network connection to a third-party system using user-controlled data for resource URI. An attacker might leverage this vulnerability to send a request on behalf of the application server since the request will originate from the application server's internal IP address.
Severity Rating	**Medium**
Impact	A Server-Side Request Forgery occurs when an attacker can influence a network connection made by the application server. The network connection will originate from the application server's internal IP and an attacker can use this connection to bypass network controls and scan or attack internal resources that are not otherwise exposed.
Recommendation	It is recommended to not establish network connections based on user-controlled data and ensure that the request is being sent to the expected destination. If user data is necessary to build the destination URI, use a level of indirection: create a list of legitimate resource names that a user is allowed to specify, and only allow the user to select from the list. With this approach the input provided by the user is never used directly to specify the resource name.
References	http://media.blackhat.com/bh-us-12/Briefings/Polyakov/BH_US_12_Polyakov_SSRF_Business_Slides.pdf
Proof of Concept:	

package_index.py

```
1069            request = urllib.request.Request(new_url)
1070            request.add_header("Authorization", auth)
1071        else:
1072            request = urllib.request.Request(url)
1073
1074        request.add_header('User-Agent', user_agent)
1075        fp = opener(request)
```

FIGURE 19: SERVER-SIDE REQUEST FORGERY

20. WEAK ENCRYPTION: INSECURE MODE OF OPERATION	
Source File	RobilityDesigner/Functions/FeatureManager/Features.cs; 132 RobilityDesigner/Functions/Robility.ServiceCall/TokenManager.cs; 254 RobilityDesigner/Functions/SmartRPAActivities/GlobalVariables.cs; 508, 587 RobilityDesigner/Functions/SmartRPAActivities/RobotFunctions.cs; 1062, 1115 RobilityDesigner/Functions/SmartRPAActivities/StringCipher.cs; 39, 81 RobilityDesigner/Robility.Launcher/AppSupportClasses/AppCommonMethods.cs; 69 RobilityDesigner/Robility.Launcher/Utilities/StringCipher.cs; 38, 80 RobilityDesigner/Robility.Launcher/ViewModel/ConnectFormViewModel.cs; 962 RobilityDesigner/Robility.Launcher/ViewModel/FileUtility.cs; 165 RobilityDesigner/SaveWorkflowDetails.cs; 55 RobilityDesigner/WorkflowServices/Service References/WorkflowServiceClient/Reference.cs; 1916 RobilityDesigner/WorkflowServices/WorkflowServices.cs; 1019, 1083 RobilityDesigner/WorkflowServices_Live/Service References/WorkflowServiceClient/Reference.cs; 1916 RobilityDesigner/WorkflowServices_Live/WorkflowServices.cs; 1029, 1093 Runner/CommonHelper/ApplicationPath.cs; 145 Runner/CommonHelper/Helper.cs; 292, 335 Runner/ProductUpdateDownloader/ProductUpdater.cs; 249 Runner/Robility.ServiceCalls/TokenManager.cs; 263 Runner/RobilityRunner/RobilityClass/StringCipher.cs; 39, 81, 119, 166 Runner/RobilityServiceLayer/Service References/CredentialService/Reference.cs; 945 Runner/RobilityServiceLayer/Service References/DesignerService/Reference.cs; 2867 Runner/RobilityServiceLayer/Service References/FeatureService/Reference.cs; 232 Runner/RobilityServiceLayer/Service References/RunnerService/Reference.cs; 458 Runner/RobilityServiceLayer/Service References/TemplateRepository/Reference.cs; 2672 Runner/SmartRPALogonService/LogonClass/DecryptAes.cs; 72 Runner/SmartRPALogonService/RobilityClass/StringCipher.cs; 39, 81, 111, 141 Runner/SmartRPALogonService/Service References/LogonService/Reference.cs; 396 Runner/SmartRPALogonService/Service References/WebService/Reference.cs; 242 RobilityActivites/Robility.AppIntegration/Common/EncryptInformation.cs; 40 RobilityActivites/Robility.CopilotControl/Common/EncryptInformation.cs; 43 RobilityActivites/Robility.CryptographyAutomation/FileUtility.cs; 81, 85 RobilityActivites/Robility.CryptographyAutomation/TextUtility.cs; 33, 42 RobilityActivites/Robility.DesktopAutomation/SecureTypeText.cs; 573 RobilityActivites/Robility.ExcelAutomation/Common/EncryptionService.cs; 47, 86 RobilityActivites/Robility.GoogleDrive/Common/EncryptInformation.cs; 40

	RobilityActivites/Robility.GoogleSheet/Robility.GoogleSheet/Common/EncryptInformation.cs; 40 RobilityActivites/Robility.Interact/Utility/EncryptInformation.cs; 36 RobilityActivites/Robility.InternetExplorer/SecureSetText.cs; 655 RobilityActivites/Robility.Manager/ApiService.cs; 314, 354 RobilityActivites/Robility.Manager/Common.cs; 42, 124 RobilityActivites/Robility.Manager/CryptoHelper.cs; 41, 77 RobilityActivites/Robility.SQliteAutomation/EncryptDecrypt.cs; 36, 126 RobilityActivites/Robility.SalesForceEmail/ApiHelper.cs; 85 RobilityActivites/Robility.SalesForceOperation/ApiHelper.cs; 83 RobilityActivites/Robility.SalesForceToken/ApiHelper.cs; 57 RobilityActivites/Robility.SmartInteract/ApplicationPath.cs; 135 RobilityActivites/Robility.SmartInteract/Common.cs; 90 RobilityActivites/Robility.Twilio/Common/EncryptInformation.cs; 42 RobilityActivites/Robility.WebAutomation/SecureSetText.cs; 2617 RobilityActivites/Robility.ZenDesk/Common/EncryptInformation.cs; 40
Observation	During assessment it was observed that the mentioned uses a cryptographic encryption algorithm with an insecure mode of operation.
Severity Rating	**Medium**
Impact	The mode of operation of a block cipher is an algorithm that describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block. Some modes of operation include Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Counter (CTR).
Recommendation	It is recommended to avoid using ECB and CBC modes of operation when encrypting data larger than a block. CBC mode is somewhat inefficient and poses a serious risk if used with SSL. Instead, use CCM (Counter with CBC-MAC) mode or, if performance is a concern, GCM (Galois/Counter Mode) mode where they are available.
References	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566

Proof of Concept:

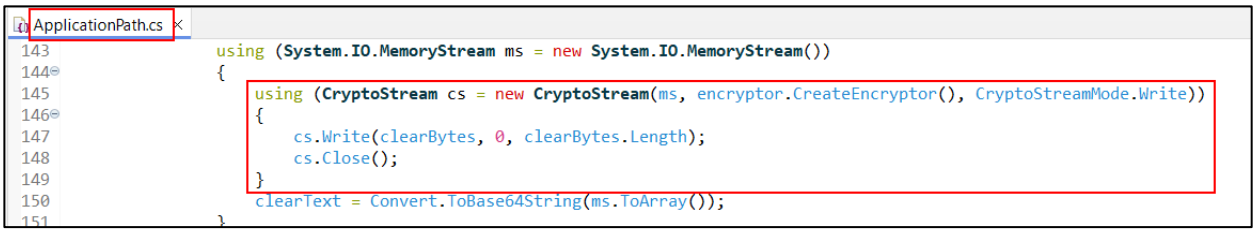


FIGURE 20: WEAK ENCRYPTION: INSECURE MODE OF OPERATION

21. XML INJECTION	
Source File	RobilityActivites/RobilityWebClient/clsFunction.cs; 361 RobilityActivites/SpyCommunicator/Utilities/AttributeDeserializer.cs; 33
Observation	During assessment it was observed that the mentioned method writes unvalidated XML input. This call could allow an attacker to inject arbitrary elements or attributes into the XML document.
Severity Rating	Medium
Impact	XML injection occurs when: 1. Data enters a program from an untrusted source. 2. The data is written to an XML document.
Recommendation	It is recommended that when writing user supplied data to XML, follow these guidelines: 1. Do not create tags or attributes with names that are derived from user input. 2. XML entity encode user input before writing to XML. 3. Wrap user input in CDATA tags.
References	https://vulncat.fortify.com/en/detail?category=XML+Injection

Proof of Concept:

AttributeDeserializer.cs

```
31          {
32              string rootedXml = "<xmlnode>" + xmlValue + "</xmlnode>";
33              XDocument xdoc = XDocument.Parse(rootedXml);
34              ObservableCollection<RootAttribute> rootAttributes = new ObservableCollection<RootAttribute>();
35              foreach (var (doc, nodeName, attribute) in from XElement doc in xdoc.Root.Descendants()
36                                                         let nodeName = doc.Name.ToString()
37                                                         let attribute = new ObservableCollection<Attributes>()
38                                                         select (doc, nodeName, attribute))
39              {
```

FIGURE 21: XML INJECTION

22. XPATH INJECTION	
Source File	RobilityDesigner/Robility.Launcher/Views/SupportClasses/VaultXmlUpdater.cs; 81
Observation	During assessment it was observed that the mentioned method invokes an XPath query built using unvalidated input. This call could allow an attacker to modify the statement's meaning or to execute arbitrary XPath queries.
Severity Rating	Medium
Impact	XPath injection occurs when: 1. Data enters a program from an untrusted source. 2. The data used to dynamically construct an XPath query.
Recommendation	It is recommended to use an allow list to ensure that user-controlled values used in an XPath query are composed from only the expected set of characters and do not contain any XPath metacharacters given the context in which they are used.
References	https://vulncat.fortify.com/en/detail?category=XPath+Injection

Proof of Concept:

VaultXmlUpdater.cs

```
77
78          // Ensure the child node exists under parent
79          private XmlNode GetOrCreateChildNode(XmlNode parentNode, string childName)
80          {
81              XmlNode child = parentNode.SelectSingleNode(childName);
82              if (child == null)
83              {
84                  child = Doc.CreateElement(childName);
85                  parentNode.AppendChild(child);
86              }
87              return child;
88          }
89
```

FIGURE 22: XPATH INJECTION

23. PATH MANIPULATION: BASE PATH OVERWRITING	
Source File	RobilityDesigner/ChildSessionRunnerInstance/Utilities/Common.cs; 20 RobilityDesigner/Execution/WorkflowDebugger.cs; 58 RobilityDesigner/Functions/ExecuteXamlWorkflow/TemplatesValidation.cs; 231, 448 RobilityDesigner/Prompt/PromptTree.cs; 33 RobilityDesigner/ReusableObjects/ViewModel/ContentPresenterExtractor.cs; 21 RobilityDesigner/Robility.Launcher/App.xaml.cs; 252 RobilityDesigner/Robility.Launcher/ManageFeatures/ManageFeatureViewModel.cs; 3106, 3190, 3410, 3755, 3756 RobilityDesigner/Robility.Launcher/Utilities/Utility.cs; 67 RobilityDesigner/Robility.Launcher/ViewModel/Assign/DefaultAssign.cs; 34, 50 RobilityDesigner/Robility.Launcher/ViewModel/DesignerLauncherViewModel.cs; 3066, 5275 RobilityDesigner/Robility.Launcher/ViewModel/OpenSolution/RenameSolution.cs; 226, 249, 266 RobilityDesigner/Robility.Launcher/Views/DesignerLauncher.xaml.cs; 315, 652, 726 RobilityDesigner/Robility.Launcher/Views/NewProject.xaml.cs; 127 RobilityDesigner/RunnerInstance/WorkflowExecution/Runner.cs; 944 RobilityDesigner/ViewModel/MainWindwoActiproViewModel.cs; 1411, 5910 RobilityDesigner/ViewModel/SolutionPropertiescontextmenus.cs; 1559 Runner/RobilityRunner/AutoConnectListener.cs; 226 RobilityActivites/Robility.AssistedVirtualSession/InvokeChildSession.cs; 117 RobilityActivites/Robility.Cognitive/AbbyyCloudOCR.cs; 372 RobilityActivites/Robility.FSAutomation/CreateFile.cs; 198, 202, 215, 219, 233, 237, 258 RobilityActivites/Robility.Invoke/InvokeDll.cs; 90 RobilityActivites/Robility.Invoke/InvokeTemplate.cs; 106, 431, 434 RobilityActivites/Robility.Invoke/InvokeWorkflow.cs; 343, 347 RobilityActivites/Robility.MailAutomation.Outlook/Clsextractmailmessage.cs; 99, 101, 122 RobilityActivites/Robility.MarkplacePythonExecution/MainWindow.xaml.cs; 98 RobilityActivites/Robility.OutlookAutomation/Clsextractmailmessage.cs; 149, 151, 172 RobilityActivites/Robility.OutlookAutomation/Save.cs; 124 RobilityActivites/Robility.FTPAutomation/clsFTP.cs; 260, 264
Observation	During assessment it was observed that the attackers can control the file system path argument, which enables them to access or modify otherwise protected files.
Severity Rating	Low
Impact	Path.Combine takes several file paths as arguments. It concatenates them to get a full path, which is typically followed by a call to read() or write() to that file.

Recommendation	It is recommended to make sure that user-controlled paths are checked to be absolute paths. You can use System.IO.Path.IsPathRooted() since it will return true for file system and UNC absolute paths.
References	https://www.praetorian.com/blog/pathcombine-security-issues-in-aspnet-applications/

Proof of Concept:

clsFTP.cs

```
256                 {
257                     Uri server = new Uri(ftpServerDirectorypath);
258                     if (CheckIfFileExistsOnServer(ftpUserID,ftpPassword,server,file))
259                     {
260                         DeleteFtpFile(ftpUserID, ftpPassword,Path.Combine(ftpServerDirectorypath, file));
261                     }
262                     else
263                     {
264                         RemoveDirectory(ftpUserID, ftpPassword,Path.Combine(ftpServerDirectorypath , file));
265                     }
266                 }
```

FIGURE 23: PATH MANIPULATION: BASE PATH OVERWRITING

24. PATH MANIPULATION: ZIP ENTRY OVERWRITE	
Source File	RobilityDesigner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 1252 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 1252
Observation	During assessment it was observed that the mentioned call enables an attacker to arbitrarily write to a file anywhere on the system.
Severity Rating	Low
Impact	Path Manipulation: Zip Entry Overwrite errors occur when a Zip file is opened and expanded without checking the file path of the Zip entry.
Recommendation	It is recommended when decompressing untrusted Zip files, make sure to use a secure version of the Zip library.
References	https://vulncat.fortify.com/en/detail?category=Path+Manipulation&subcategory=Zip+Entry+Overwrite

Proof of Concept:

util.py

```
1248                # bytes -> unicode conversion using ASCII to decode.
1249                for tarinfo in archive.getmembers():
1250                    if not isinstance(tarinfo.name, text_type):
1251                        tarinfo.name = tarinfo.name.decode('utf-8')
1252            archive.extractall(dest_dir)
1253
1254        finally:
1255            if archive:
1256                archive.close()
```

FIGURE 24: PATH MANIPULATION: ZIP ENTRY OVERWRITE

25. SYSTEM INFORMATION LEAK: EXTERNAL	
Source File	RobilityDesigner/Functions/ElementEditor/Views/ElementEditorView.xaml.cs; 333 RobilityDesigner/Robility.Launcher/ViewModel/DesignerLauncherViewModel.cs; 2117 RobilityActivites/FlaUInspect/Models/FileOperation.cs; 26 RobilityActivites/JavaSpy/PropertyListView/FileOperation.cs; 30 RobilityActivites/ModernDesktopSpy/Models/FileOperation.cs; 31 RobilityActivites/Robility.DesktopAutomationUIA3/OpenSpyApplication.cs; 178 RobilityActivites/Robility.JavaApp/OpenSpyApplication.cs; 128 RobilityActivites/Robility.ModernDesktopAutomation/OpenSpyApplication.cs; 145 RobilityActivites/Robility.RecorderUI/Robility.RecorderUI/ViewModels/RecordedActionsViewModelWithHelper.cs; 316 RobilityActivites/Robility.Interact/GetMasterData.cs; 243 RobilityActivites/lbmeghcehlmclgjmnefeflchpbdblamd/1.5_0/scripts/contentScript.js; 133 RobilityActivites/lbmeghcehlmclgjmnefeflchpbdblamd/lbmeghcehlmclgjmnefeflchpbdblamd/scripts/contentScript.js; 133
Observation	During assessment it was observed that the mentioned function might reveal system data or debug information by calling alert(). The information revealed by alert() could enable an adversary to plan an attack.
Severity Rating	Low
Impact	An external information leak occurs when system data or debug information leaves the program to a remote machine via a socket or network connection. External leaks can help an attacker by revealing specific data about operating systems, full pathnames, the existence of usernames, or locations of configuration files, and are more serious than internal information leaks, which are more difficult for an attacker to access.
Recommendation	It is recommended to write error messages with security in mind. In production environments, turn off detailed error information in favour of brief messages.
References	https://vulncat.fortify.com/en/detail?category=System+Information+Leak&subcategory=External

Proof of Concept:

FileOperation.cs

```
19          {
20              if (!Directory.Exists(filepath))
21              {
22                  Directory.CreateDirectory(filepath);
23              }
24              String filename = filepath + "\\SpiedValue.txt";
25
26              System.IO.File.WriteAllText(filename, SpiedValue);
27
28          }
```

FIGURE 25: SYSTEM INFORMATION LEAK: EXTERNAL

26. WCF MISCONFIGURATION: ANONYMOUS TRANSPORT CLIENT	
Source File	RobilityDesigner/App.config; 43, 51, 68, 95, 102, 109 RobilityDesigner/ChildSessionRunnerInstance.exe.config; 24, 32, 58, 65 RobilityDesigner/ChildSessionRunnerInstance/App.config; 24, 32, 40, 49 RobilityDesigner/Dlls/RobilityRoboPoster.exe.config; 11, 17 RobilityDesigner/Functions/DesignerDebugger/App.config; 43, 51, 68, 95, 102 RobilityDesigner/Functions/ProductUpdateDownloader/App.config; 26, 34, 41, 52, 59 RobilityDesigner/Functions/ProductUpdater/App.config; 26, 34, 41, 52, 59 RobilityDesigner/Robility.Launcher/App.config; 28, 36, 53, 80, 87 RobilityDesigner/RobilityRoboPoster/RobilityRoboPoster/App.config; 43, 51, 60, 67, 94, 101 RobilityDesigner/RobilityRunner/App.config; 19, 27, 35, 44 RobilityDesigner/RunnerInstance/App.config; 19, 27, 35, 44 RobilityDesigner/SmartRunnerInstance.exe.config; 19, 27, 42, 59 RobilityDesigner/WorkflowServices/App.config; 44 RobilityDesigner/WorkflowServices_Live/App.config; 42 Runner/ProductUpdateDownloader/App.config; 23, 31, 38, 49, 56 Runner/ProductUpdater/App.config; 26, 34, 41, 52, 59 Runner/RobilityAssistedRobot/App.config; 28, 35, 43, 51 Runner/RobilityRunner/App.config; 35, 43, 51, 60 Runner/RobilityRunner/SmartRPALogon/RobilityLogon.exe.config; 32, 38 Runner/RobilityRunner/SmartRPALogon/SmartRPALogon.exe.config; 32, 38 Runner/RobilityServiceLayer/app.config; 9, 17, 23, 29, 35, 41 Runner/RunnerInstance/App.config; 19, 27, 35, 44 Runner/SmartRPALogonService/App.config; 32, 38 RobilityActivites/Robility.DesktopAutomation/app.config; 8 RobilityActivites/Robility.DesktopAutomationUIA3/app.config; 8 RobilityActivites/Robility.DesktopAutomation_Production/app.config; 8 RobilityActivites/Robility.InternetExplorer/app.config; 8 RobilityActivites/Robility.InternetExplorer_Production/app.config; 8 RobilityActivites/Robility.JavaApp/app.config; 8 RobilityActivites/Robility.KeyBoardAutomation/app.config; 8 RobilityActivites/Robility.Manager/app.config; 8 RobilityActivites/Robility.SmartInteract/app.config; 8 RobilityActivites/Robility.WebAutomation/app.config; 8 RobilityActivites/Robility.WebAutomation_V3/app.config; 8
Observation	During assessment it was observed that the absence of authentication means everyone is able to access this service.
Severity Rating	Low
Impact	A service that does not authenticate its clients allows all comers to access its functionality.

Recommendation	It is recommended to configure the application to authenticate against client credentials.
References	http://msdn.microsoft.com/en-us/library/ms730301.aspx

Proof of Concept:

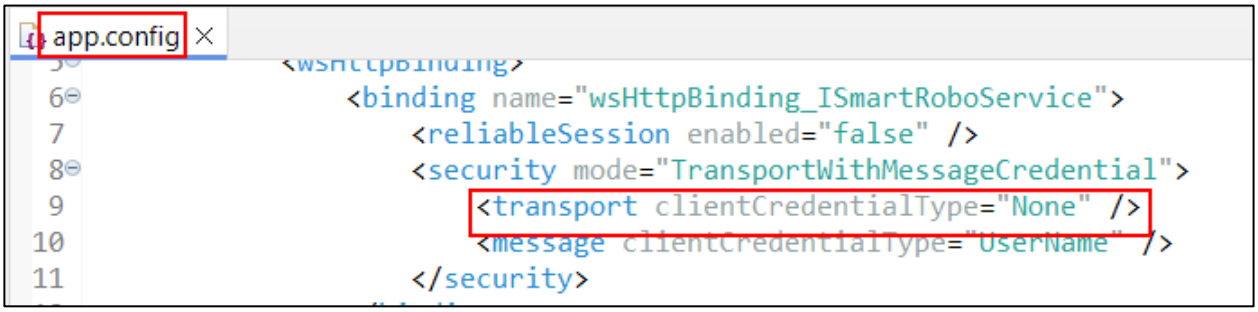


FIGURE 26: WCF MISCONFIGURATION: ANONYMOUS TRANSPORT CLIENT

27. WCF MISCONFIGURATION: INSUFFICIENT LOGGING

Source File	RobilityDesigner/App.config; 123 RobilityDesigner/ChildSessionRunnerInstance.exe.config; 95 RobilityDesigner/ChildSessionRunnerInstance/App.config; 80 RobilityDesigner/Functions/DesignerDebugger/App.config; 116 RobilityDesigner/Functions/ProductUpdateDownloader/App.config; 73 RobilityDesigner/Functions/ProductUpdater/App.config; 73 RobilityDesigner/Robility.Launcher/App.config; 101 RobilityDesigner/RobilityRoboPoster/RobilityRoboPoster/App.config; 115 RobilityDesigner/RobilityRunner/App.config; 75 RobilityDesigner/RunnerInstance/App.config; 75 RobilityDesigner/SmartRunnerInstance.exe.config; 90 Runner/ProductUpdateDownloader/App.config; 70 Runner/ProductUpdater/App.config; 73 Runner/RobilityAssistedRobot/App.config; 73 Runner/RobilityRunner/App.config; 91 Runner/RunnerInstance/App.config; 75
Observation	During assessment it was observed that the lack of a proper audit trail after a security incident can hamper forensic efforts.
Severity Rating	Low
Impact	Windows Communication Foundation (WCF) offers the ability to log successful and/or failed authentication attempts. Logging failed authentication attempts can warn administrators of potential brute-force attacks.
Recommendation	It is recommended to enable WCF's service security audit feature.
References	http://msdn.microsoft.com/en-us/library/ms731694.aspx

Proof of Concept:

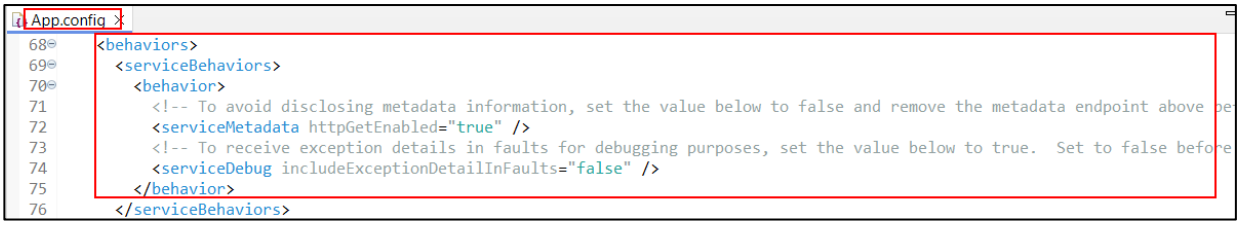


FIGURE 27: WCF MISCONFIGURATION: INSUFFICIENT LOGGING

28. WCF MISCONFIGURATION: SERVICE ENUMERATION

Source File	RobilityDesigner/App.config; 125 RobilityDesigner/ChildSessionRunnerInstance.exe.config; 97 RobilityDesigner/ChildSessionRunnerInstance/App.config; 82 RobilityDesigner/Functions/DesignerDebugger/App.config; 118 RobilityDesigner/Functions/ProductUpdateDownloader/App.config; 75 RobilityDesigner/Functions/ProductUpdater/App.config; 75 RobilityDesigner/Robility.Launcher/App.config; 103 RobilityDesigner/RobilityRoboPoster/RobilityRoboPoster/App.config; 117 RobilityDesigner/RobilityRunner/App.config; 77 RobilityDesigner/RunnerInstance/App.config; 77 RobilityDesigner/SmartRunnerInstance.exe.config; 92 Runner/ProductUpdateDownloader/App.config; 72 Runner/ProductUpdater/App.config; 75 Runner/RobilityAssistedRobot/App.config; 75 Runner/RobilityRunner/App.config; 93 Runner/RunnerInstance/App.config; 77
Observation	During assessment it was observed that publicly exposing information about a service can provide attackers with valuable insight into how they might exploit the service.
Severity Rating	Low
Impact	The <serviceMetadata> tag enables the metadata publishing feature. Service metadata could contain sensitive information that should not be publicly accessible.
Recommendation	It is recommended to only allow trusted users to access the metadata and ensure that unnecessary information is not exposed. Better yet, entirely disable the ability to publish metadata. A safe WCF configuration will not contain the <serviceMetadata> tag.
References	http://msdn.microsoft.com/en-us/library/ms731317.aspx

Proof of Concept:

App.config

```
68    <behaviors>
69      <serviceBehaviors>
70        <behavior>
71          <!-- To avoid disclosing metadata information, set the value below to false and remove the metadata endpoint abo
72          <serviceMetadata httpGetEnabled="true" />
73          <!-- To receive exception details in faults for debugging purposes, set the value below to true.  Set to false b
74          <serviceDebug includeExceptionDetailInFaults="false" />
75        </behavior>
```

FIGURE 28: WCF MISCONFIGURATION: SERVICE ENUMERATION

29. WCF MISCONFIGURATION: WEAK TOKEN	
Source File	RobilityDesigner/App.config; 44, 52, 69, 96, 103, 110 RobilityDesigner/ChildSessionRunnerInstance.exe.config; 25, 33, 59, 66 RobilityDesigner/ChildSessionRunnerInstance/App.config; 25, 33, 41, 50 RobilityDesigner/Dlls/RobilityRoboPoster.exe.config; 12, 18 RobilityDesigner/Functions/DesignerDebugger/App.config; 44, 52, 69, 96, 103 RobilityDesigner/Functions/ProductUpdateDownloader/App.config; 27, 35, 42, 53, 60 RobilityDesigner/Functions/ProductUpdater/App.config; 27, 35, 42, 53, 60 RobilityDesigner/Robility.Launcher/App.config; 29, 37, 54, 81, 88 RobilityDesigner/RobilityRoboPoster/RobilityRoboPoster/App.config; 44, 52, 61, 68, 95, 102 RobilityDesigner/RobilityRunner/App.config; 20, 28, 36, 45 RobilityDesigner/RunnerInstance/App.config; 20, 28, 36, 45 RobilityDesigner/SmartRunnerInstance.exe.config; 20, 28, 43, 60 RobilityDesigner/WorkflowServices/App.config; 45 RobilityDesigner/WorkflowServices_Live/App.config; 43 Runner/ProductUpdateDownloader/App.config; 24, 32, 39, 50, 57 Runner/ProductUpdater/App.config; 27, 35, 42, 53, 60 Runner/RobilityAssistedRobot/App.config; 29, 36, 44, 52 Runner/RobilityRunner/App.config; 36, 44, 52, 61 Runner/RobilityRunner/SmartRPALogon/RobilityLogon.exe.config; 33, 39 Runner/RobilityRunner/SmartRPALogon/SmartRPALogon.exe.config; 33, 39 Runner/RobilityServiceLayer/app.config; 10, 18, 24, 30, 36, 42 Runner/RunnerInstance/App.config; 20, 28, 36, 45 Runner/SmartRPALogonService/App.config; 33, 39 RobilityActivites/Robility.DesktopAutomation/app.config; 9 RobilityActivites/Robility.DesktopAutomationUIA3/app.config; 9 RobilityActivites/Robility.DesktopAutomation_Production/app.config; 9 RobilityActivites/Robility.InternetExplorer/app.config; 9 RobilityActivites/Robility.InternetExplorer_Production/app.config; 9 RobilityActivites/Robility.JavaApp/app.config; 9 RobilityActivites/Robility.KeyBoardAutomation/app.config; 9 RobilityActivites/Robility.Manager/app.config; 9 RobilityActivites/Robility.SmartInteract/app.config; 9 RobilityActivites/Robility.WebAutomation/app.config; 9 RobilityActivites/Robility.WebAutomation_V3/app.config; 9
Observation	During assessment it was observed that Service Providers that use the UsernameToken might accept passwords sent in plain text.
Severity Rating	Low
Impact	Using a UsernameToken with a plain text password over an unencrypted channel exposes the password to attackers who can sniff the SOAP messages.

Recommendation	It is recommended to Set clientCredentialType to Certificate or Windows.
References	https://vulncat.fortify.com/en/detail?category=WCF+Misconfiguration&subcategory=Weak+Token

Proof of Concept:

app.config

```
4        <bindings>
5            <wsHttpBinding>
6                <binding name="wsHttpBinding_ISmartRoboService">
7                    <reliableSession enabled="false" />
8                    <security mode="TransportWithMessageCredential">
9                        <transport clientCredentialType="None" />
10                       <message clientCredentialType="UserName" />
11                   </security>
12               </binding>
```

FIGURE 29: WCF MISCONFIGURATION: WEAK TOKEN

30. DENIAL OF SERVICE	
Source File	RobilityDesigner/Functions/FeatureManager/Features.cs; 141 RobilityDesigner/Functions/GitLeaksScannerLib/GitLeaksScanner.cs; 315, 316 RobilityDesigner/Functions/Robility.DebugTracking/VisualTracking.cs; 619 RobilityDesigner/Functions/RobilityActivityTray/TrayPipeListener.cs; 177 RobilityDesigner/Functions/SmartRPAActivities/GlobalVariables.cs; 356 RobilityDesigner/Functions/SmartRPAActivities/StringCipher.cs; 90 RobilityDesigner/ObjectRepository/RespositoryParser.cs; 42 RobilityDesigner/ReusableObjects/ViewModel/ReusableObjectViewModel.cs; 360 RobilityDesigner/Robility.Launcher/AppSupportClasses/AppCommonMethods.cs; 89 RobilityDesigner/Robility.Launcher/Extension/Utility.cs; 36 RobilityDesigner/Robility.Launcher/Utilities/StringCipher.cs; 89 RobilityDesigner/Robility.Launcher/Utilities/Utility.cs; 39 RobilityDesigner/Robility.Launcher/ViewModel/ConnectFormViewModel.cs; 982 RobilityDesigner/RobilityRunner/Program.cs; 150 RobilityDesigner/RobilityRunner/WorkflowExecution/Runner.cs; 656 RobilityDesigner/RunnerExecution/RunnerInstanceExecution.cs; 559 RobilityDesigner/RunnerInstance/Utilities/ActivityTrayBridge.cs; 211 RobilityDesigner/UIExplore/PluginsHandlers/BrowserSpyCommunicator.cs; 66 RobilityDesigner/Utilities/Utility.cs; 35 RobilityDesigner/ViewModel/DllImports.cs; 636 RobilityDesigner/ViewModel/Importfiles.cs; 498, 535, 649 RobilityDesigner/WorkflowServices/WorkflowServices.cs; 314 RobilityDesigner/WorkflowServices_Live/WorkflowServices.cs; 314 Runner/ProductUpdateDownloader/ProductUpdater.cs; 258 Runner/RobilityRunner/RobilityClass/StringCipher.cs; 90, 175 Runner/SmartRPALogonService/LogonClass/DecryptAes.cs; 95 Runner/SmartRPALogonService/RobilityClass/StringCipher.cs; 90, 150 RobilityActivites/ChromeSpy - Copy/AdvanceSpyWindow.xaml.cs; 196 RobilityActivites/ChromeSpy - Copy/MainWindow.xaml.cs; 172 RobilityActivites/ChromeSpy - Copy/View/AdvancedSpyWindow.xaml.cs; 128 RobilityActivites/ChromeSpy - Copy/View/SpyWindow.xaml.cs; 129 RobilityActivites/ChromeSpy/AdvanceSpyWindow.xaml.cs; 205 RobilityActivites/ChromeSpy/MainWindow.xaml.cs; 211 RobilityActivites/ChromeSpy/View/AdvancedSpyWindow.xaml.cs; 128 RobilityActivites/ChromeSpy/View/SpyWindow.xaml.cs; 129 RobilityActivites/Robility.AzureKeyvault/Common.cs; 165 RobilityActivites/Robility.Cognitive/Designer/dsGoogleVisionOCR.xaml.cs; 109 RobilityActivites/Robility.Cognitive/ImageOptimization.cs; 66 RobilityActivites/Robility.CoreActivities/InvokeVBScript.cs; 128, 129 RobilityActivites/Robility.CryptographyAutomation/FileUtility.cs; 146 RobilityActivites/Robility.DesktopAutomation/SecureTypeText.cs; 595

	RobilityActivites/Robility.DesktopAutomationUIA3/Utilities/Common.cs; 181 RobilityActivites/Robility.FTPAutomation/clsFTP.cs; 228 RobilityActivites/Robility.GoogleCognitiveServices/Designer/dsVisionOCR.xaml.cs; 55 RobilityActivites/Robility.GoogleCognitiveServices/VisionOCR.cs; 769 RobilityActivites/Robility.GoogleSheet/Robility.GoogleSheet/CreateSpreadSheet.cs; 110 RobilityActivites/Robility.Interact/Utility/UtilitiesAddTransaction.cs; 82 RobilityActivites/Robility.InternetExplorer/Clsutility.cs; 152 RobilityActivites/Robility.InternetExplorer/SecureSetText.cs; 677 RobilityActivites/Robility.InternetExplorer/Utilities/MouseHoverRuntime.cs; 54 RobilityActivites/Robility.InternetExplorer_Production/Clsutility.cs; 166 RobilityActivites/Robility.InternetExplorer_Production/MouseHover.cs; 385 RobilityActivites/Robility.Invoke/InvokeWorkflow.cs; 229 RobilityActivites/Robility.KeyBoardAutomation/SendTextData.cs; 206 RobilityActivites/Robility.KeyBoardAutomation/SendTextPartial.cs; 98, 100, 131, 133, 135, 138 RobilityActivites/Robility.MailAutomation.Outlook/OutlookStorage.cs; 1021 RobilityActivites/Robility.Manager/Common.cs; 159 RobilityActivites/Robility.Marketplace/PythonScriptLoader.cs; 441 RobilityActivites/Robility.Marketplace/PythonVirtualEnvironement.cs; 171 RobilityActivites/Robility.MicrosoftCognitiveServices/Designer/dsVisionOCR.xaml.cs; 56 RobilityActivites/Robility.MicrosoftCognitiveServices/ImageOptimization.cs; 66 RobilityActivites/Robility.MicrosoftOutlook365/Common/ClsUtilities.cs; 84 RobilityActivites/Robility.NLTKEntityextraction/NLTKNamedentityExtraction.cs; 130 RobilityActivites/Robility.OSFunctionsAutomation/ReadText.cs; 99 RobilityActivites/Robility.OutlookAutomation/OutlookStorage.cs; 988 RobilityActivites/Robility.PythonAutomation/InvokeScript.cs; 43, 46 RobilityActivites/Robility.RecorderUI/Robility.RecorderUI/Services/RecordingXmlService.cs; 36 RobilityActivites/Robility.RecorderUI/Robility.RecorderUI/ViewModels/RecordedActionsViewModelWithHelper.cs; 222 RobilityActivites/Robility.Recorders/Runtime/TestCaseExecutor.cs; 184 RobilityActivites/Robility.SAPAutomation/ExtractTableHelper.cs; 154 RobilityActivites/Robility.SAPAutomation/SapInvoke.cs; 107, 108 RobilityActivites/Robility.SAPAutomation/ScriptExecutor.cs; 58, 80 RobilityActivites/Robility.SQliteAutomation/DBBackup.cs; 204, 207 RobilityActivites/Robility.SQliteAutomation/ExportCSV.cs; 232, 234 RobilityActivites/Robility.SQliteAutomation/ImportData.cs; 1062, 1064 RobilityActivites/Robility.Terminal/Common/ConnectNamedPipe.cs; 172 RobilityActivites/Robility.TextAutomation/AppendText.cs; 131 RobilityActivites/Robility.TextAutomation/ReadText.cs; 118 RobilityActivites/Robility.WebAutomation/SecureSetText.cs; 2639

	RobilityActivites/Robility.WebAutomation/frmInjectJS.cs; 60 RobilityActivites/Robility.WebAutomation_V3/frmInjectJS.cs; 60 RobilityActivites/RobilityWebClient/ClsUtilities.cs; 88 RobilityActivites/RobilityWebClient/Designer/SoapClientUISplited.cs; 359 RobilityActivites/RobilityWebClient/RestConsumerPartial.cs; 117 RobilityActivites/RobilityWebClient/Soap.cs; 519 RobilityActivites/RobilityWebClient/clsFunction.cs; 360, 387 RobilityActivites/SpyCommunicator/WebSpyCommunication/FileWatcherCls.cs; 101 RobilityActivites/UIExplore/PluginsHandlers/BrowserSpyCommunicator.cs; 66 RobilityActivites/UIExplore/UIExplore/PluginsHandlers/BrowserSpyCommunicator.cs; 64 RobilityActivites/UIExplore/UIExplore/SpyClass/FindWebElement.cs; 385 RobilityActivites/WebCommunicator/FileWatcher/FileWatcherCls.cs; 88
Observation	During assessment it was observed that the mentioned call might allow an attacker to crash the program or otherwise make it unavailable to legitimate users.
Severity Rating	Low
Impact	Attackers may be able to deny service to legitimate users by flooding the application with requests, but flooding attacks can often be defused at the network layer. More problematic are bugs that allow an attacker to overload the application using a small number of requests. Such bugs allow the attacker to specify the quantity of system resources their requests will consume or the duration for which they will use them.
Recommendation	It is recommended to validate user input to ensure that it will not cause inappropriate resource utilization.
References	https://vulncat.fortify.com/en/detail?category=Denial+of+Service

Proof of Concept:

DecryptAes.cs

```
90
91                          using (var srDecrypt = new StreamReader(csDecrypt))
92                          {
93                              // Read the decrypted bytes from the decrypting stream
94                              // and place them in a string.
95                              plaintext = srDecrypt.ReadToEnd();
96
97                          }
```

FIGURE 30: DENIAL OF SERVICE

31. DENIAL OF SERVICE: REGULAR EXPRESSION	
Source File	RobilityActivites/Robility.AdvancedWebAutomation/HTMLTableToDataTable.cs; 365, 383 RobilityActivites/Robility.MailAutomation.Outlook/Save.cs; 79 RobilityActivites/Robility.OutlookAutomation/Save.cs; 87 RobilityActivites/Robility.RegEx/RegexBuilderDatas/RegexWindowViewModel.cs; 148 RobilityActivites/Robility.WebAutomation/HTMLTableToDataTable.cs; 386, 404
Observation	During assessment it was observed that untrusted data is passed to the application and used as a regular expression. This can cause the thread to overconsume CPU resources.
Severity Rating	Low
Impact	There is a vulnerability in implementations of regular expression evaluators and related methods that can cause the thread to hang when evaluating regular expressions that contain a grouping expression that is itself repeated
Recommendation	It is recommended to not allow untrusted data to be used as regular expression patterns. If this solution is impractical for your application, Microsoft recommends to set the matchTimeout parameter to an appropriate value, such as two seconds.
References	https://msdn.microsoft.com/en-us/library/gg578045(v=vs.110).aspx#Timeouts

Proof of Concept:

HTMLTableToDataTable.cs

```
361                 bool HeadersExist = false;
362                 int iCurrentRow = 0;
363
364                 // Get a match for all the tables in the HTML
365                 MatchCollection Tables = Regex.Matches(HTML, TableExpression, RegexOptions.Multiline | RegexOptions.Singleline
366
367                 // Loop through each table element
```

FIGURE 31: DENIAL OF SERVICE: REGULAR EXPRESSION

32. HEADER MANIPULATION	
Source File	RobilityActivites/Robility.AmazonRekognition/AmazonScope.cs; 81 RobilityActivites/Robility.AmazonS3/AmazonS3Scope.cs; 81 RobilityActivites/Robility.FacePlusPlus/FppScope.cs; 84 RobilityActivites/Robility.MySqlAutomation/ExecuteQuery.cs; 158 RobilityActivites/Robility.OutlookAutomation/OutlookScope.cs; 75, 76 RobilityActivites/RobilityWebClient/RestConsumer.cs; 91 RobilityActivites/RobilityWebClient/clsFunction.cs; 301, 336, 695
Observation	During assessment it was observed that the mentioned method includes unvalidated data in an HTTP response header. This enables attacks such as cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation or open redirect.
Severity Rating	Low
Impact	As with many software security vulnerabilities, Header Manipulation is a means to an end, not an end in itself. At its root, the vulnerability is straightforward: an attacker passes malicious data to a vulnerable application, and the application includes the data in an HTTP response header.
Recommendation	It is recommended to ensure that input validation occurs in the required places and checks for the correct properties.
References	https://dl.packetstormsecurity.net/papers/general/whitepaper_httpresponse.pdf

Proof of Concept:

AmazonS3Scope.cs

```
76
77      if ((!string.IsNullOrEmpty(AKID)) && (!string.IsNullOrEmpty(SAKey)) && (!string.IsNullOrEmpty(REPoint)))
78      {
79          context.Properties.Add("AmazonAKID", AKID);
80          context.Properties.Add("AmazonSAKey", SAKey);
81          context.Properties.Add("AmazonREPoint", REPoint);
82      }
```

FIGURE 32: HEADER MANIPULATION

33. MISSING XML VALIDATION	
Source File	RobilityActivites/RobilityWebClient/Designer/RestuiSubClass.cs; 325 RobilityActivites/RobilityWebClient/Designer/SoapClientUISplited.cs; 87 RobilityActivites/RobilityWebClient/RestConsumerPartial.cs; 251 RobilityActivites/RobilityWebClient/Soap.cs; 453
Observation	During assessment it was observed that the mentioned method fails to enable validation before using XML, which gives an attacker the opportunity to supply malicious input.
Severity Rating	Low
Impact	Most successful attacks begin with a violation of the programmer's assumptions. By accepting an XML document without validating it against a DTD or XML schema, the programmer leaves a door open for attackers to provide unexpected, unreasonable, or malicious input. It is not possible for an XML parser to validate all aspects of a document's content; a parser cannot understand the complete semantics of the data.
Recommendation	It is recommended to always enable validation when you parse XML. If enabling validation causes problems because the rules for defining a well-formed document are Byzantine or altogether unknown, chances are good that there are security errors nearby.
References	http://msdn.microsoft.com/en-us/library/system.xml.xmlvalidatingreader.aspx

Proof of Concept:

RestuiSubClass.cs

```
321                     DataSet ds = new DataSet
322                     {
323                         Locale = CultureInfo
324                     };
325                     ds.ReadXml(new XmlTextReader(new StringReader(strInput)));
326                     resultDataFormated = ds;
327                 }
```

FIGURE 33: MISSING XML VALIDATION

34. OFTEN MISUSED: AUTHENTICATION	
Source File	RobilityDesigner/ViewModel/SupportPublish/PublishObjectHelper.cs; 35, 82 Runner/CommonHelper/Helper.cs; 136
Observation	During assessment it was observed that the information returned by the mentioned call not trustworthy. Attackers may spoof DNS entries. Do not rely on DNS for security.
Severity Rating	Low
Impact	Many DNS servers are susceptible to spoofing attacks, so you should assume that your software will someday run in an environment with a compromised DNS server. If attackers are allowed to make DNS updates (sometimes called DNS cache poisoning), they can route your network traffic through their machines or make it appear as if their IP addresses are part of your domain. Do not base the security of your system on DNS names.
Recommendation	It is recommended that You can increase confidence in a domain name lookup if you check to make sure that the host's forward and backward DNS entries match. Attackers will not be able to spoof both the forward and the reverse DNS entries without controlling the nameservers for the target domain. This is not a foolproof approach however: attackers may be able to convince the domain registrar to turn over the domain to a malicious nameserver. Basing authentication on DNS entries is simply a risky proposition.
References	https://vulncat.fortify.com/en/detail?category=Often+Misused&subcategory=Authentication

Proof of Concept:

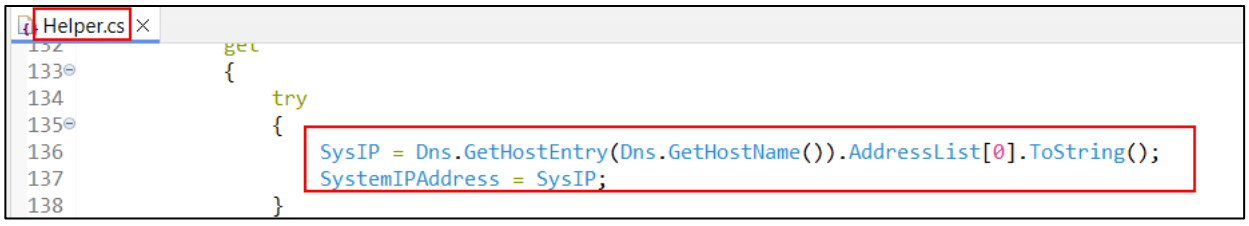


FIGURE 34: OFTEN MISUSED: AUTHENTICATION

35. PASSWORD MANAGEMENT: LACK OF KEY DERIVATION FUNCTION	
Source File	RobilityDesigner/Python/Lib/site-packages/pip/_vendor/requests/auth.py; 164, 172 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/requests/auth.py; 164, 172
Observation	During assessment it was observed that a cryptographic hash function is used to create a digest for a password.
Severity Rating	Low
Impact	A cryptographic hash function is a one-way function that is considered practically impossible to invert; that is, to recreate the input data from its digest value alone. These hash functions were considered safe to store passwords in the past because even if an attacker could access the digest value for the original password, they wouldn't be able to recover the original password from the digest value.
Recommendation	It is recommended to slow down the password hash generation process so attackers are not able to use brute-force techniques, use a Password-Based Key Derivation Function (PBKDF) instead of a cryptographic hash function.
References	http://en.wikipedia.org/wiki/Key_derivation_function

Proof of Concept:

auth.py

```
143        if _algorithm == "MD5" or _algorithm == "MD5-SESS":
144
145            def md5_utf8(x):
146                if isinstance(x, str):
147                    x = x.encode("utf-8")
148                return hashlib.md5(x).hexdigest()
149
```

FIGURE 35: PASSWORD MANAGEMENT: LACK OF KEY DERIVATION FUNCTION

36. PASSWORD MANAGEMENT:NULL PASSWORD	
Source File	RobilityDesigner/Functions/SmartRPAActivities/GlobalVariables.cs; 541 RobilityDesigner/Python/Lib/site-packages/pip/_internal/network/auth.py; 481 RobilityDesigner/Python/Lib/site-packages/pip/_internal/vcs/versioncontrol.py; 443 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 811 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/requests/sessions.py; 325 RobilityDesigner/SaveWorkflowDetails.cs; 81 RobilityDesigner/WorkflowServices/WorkflowServices.cs; 1043, 1105 RobilityDesigner/WorkflowServices_Live/WorkflowServices.cs; 1053, 1115 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/network/auth.py; 481 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/vcs/versioncontrol.py; 443 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 811 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/requests/sessions.py; 325 RobilityActivites/Robility.ExcelAutomation.Tests/BusinessLayer/FilterPivotTableTests.cs; 80, 108, 132, 159, 185, 218, 247 RobilityActivites/Robility.ExcelAutomation.Tests/BusinessLayer/UpdateAxisTitleTests.cs; 62 RobilityActivites/Robility.ExcelAutomation/InsertChart.cs; 144 RobilityActivites/Robility.PDFAutomation.Tests/BusinessLayer/ExtractImagesFromPdfUtilityTest.cs; 112
Observation	During assessment it was observed null passwords can compromise system security in a way that is difficult to remedy.
Severity Rating	Low
Impact	Assigning null to password variables is never a good idea as it may allow attackers to bypass password verification or might indicate that resources are protected by an empty password.
Recommendation	It is recommended to always read stored password values from encrypted, external resources and assign password variables meaningful values. Ensure that sensitive resources are never protected with empty or null passwords.
References	https://vulncat.fortify.com/en/detail?category=Password+Management&subcategory=Null+Password
Proof of Concept:	

auth.py

```
479             return resp
480
481         username, password = None, None
482
483          # Query the keyring for credentials:
```

FIGURE 36: PASSWORD MANAGEMENT: NULL PASSWORD

37. PASSWORD MANAGEMENT: PASSWORD IN COMMENT	
Source File	RobilityAzureServicesExecution/NamedPipe/NamedPipeServer.cs; 40 RobilityWebClient/RestConsumer.cs; 211,221
Observation	During assessment it was observed that storing passwords or password details in plain text anywhere in the system or system code might compromise system security in a way that is not easy to remedy.
Severity Rating	Low
Impact	It is never a good idea to hardcode a password. Storing password details within comments is equivalent to hardcoding passwords. Not only is the password visible to the project's developers, it also makes fixing the problem extremely difficult. After the code is in production, the password is now leaked to the outside world and cannot be protected or changed without patching the software. If the account protected by the password is compromised, the owners of the system must choose between security and availability.
Recommendation	It is recommended that passwords should never be hardcoded and should generally be obfuscated and managed in an external source. Storing passwords in plain text anywhere on the system allows anyone with sufficient permissions to read and potentially misuse the password.
References	https://vulncat.fortify.com/en/detail?category=Password+Management&subcategory=Password+in+Comment

Proof of Concept:

NamedPipeServer.cs

```
36              #region For check execution
37              //RobilityAzureServicesProperties.AzureSecretProperties azureSecretProperties = new RobilityA
38              //azureSecretProperties.Methodname = "PermanentDeleteSecret";
39              //azureSecretProperties.Clientid = "7fbc5b73-766e-46c8-abf8-478c43dfa77a";
40              //azureSecretProperties.Clientsecret = "Z4m8Q~Mr9kKe_RUATY--GDUwNvCLhZa9B2CFWa1.";
41              //azureSecretProperties.Tenantid = "9b47157b-2ccc-421f-99e7-3b3574ab942";
42              //azureSecretProperties.Keyvaulturivaue = "https://wusazerobility.vault.azure.net/";
43              //azureSecretProperties.Secretname = "TestSubbu11";
44              //azureSecretProperties.Secretvalue = "TestSubbu11";
45              //azureSecretProperties.Methodtype = RobilityAzureServicesProperties.OpMethodType.Normal;
46
```

FIGURE 37: PASSWORD MANAGEMENT: PASSWORD IN COMMENT

38. POOR LOGGING PRACTICE: USE OF A SYSTEM OUTPUT STREAM	
Source File	RobilityDesigner/Execution/WorkflowRunner.cs; 162 RobilityDesigner/Functions/ScreenEx/ScreenEx/ExternalWindow.cs; 18 RobilityDesigner/Functions/ScreenEx/ScreenEx/ScreenSize.cs; 40, 41 RobilityDesigner/Functions/SmartRPAActivities/InvokeDGLoad.xaml.cs; 991, 1018, 1053, 1105 RobilityDesigner/Functions/SmartRPAActivities/RobotFunctions.cs; 266 RobilityDesigner/Functions/SmartSpy/AutomationSpyExtension.cs; 101, 116, 134, 153, 168, 183, 199, 219, 316, 339, 353, 367, 381, 395, 409, 432, 465, 602, 1491, 1503, 1536, 1549, 1562, 1575, 1588, 1601, 1614, 1647, 1660, 1673, 1686, 1699, 1712, 1725, 1738, 1751, 1764, 1777, 1790, 1803, 1816, 1829, 1862, 1875, 1908, 1921, 1951, 1964, 1997, 2018, 2082, 2088, 2145, 2151, 2227, 2255, 2346, 2380 RobilityDesigner/Functions/SmartSpy/Event.cs; 37, 87, 105, 257, 286, 296, 305, 314, 323, 332, 341, 350, 359, 368, 377, 386, 395, 404, 413, 427, 439, 451, 474, 487, 496, 505, 514, 523, 532, 541, 550, 559, 568, 577, 586, 595, 604, 613, 628, 649, 661, 894 RobilityDesigner/Functions/SmartSpy/MainWindow.xaml.cs; 45, 64, 166, 475, 998, 1155, 1196, 1265, 1377 RobilityDesigner/Python/Lib/site-packages/pip/_internal/cli/main.py; 66, 67 RobilityDesigner/Python/Lib/site-packages/pip/_internal/cli/main_parser.py; 109, 110 RobilityDesigner/Python/Lib/site-packages/pip/_internal/commands/completion.py; 118 RobilityDesigner/Python/Lib/site-packages/pip/_internal/commands/freeze.py; 107 RobilityDesigner/Python/Lib/site-packages/pip/_internal/utils/entrypoints.py; 35 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 1705, 1707, 1724 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/pyparsing/core.py; 5911, 5915, 5917 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/rich/style.py; 730 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/ccompiler.py; 1035 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/core.py; 206 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/dist.py; 252 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/text_file.py; 153 RobilityDesigner/Python/Lib/site-packages/wheel/macosx_libfile.py; 412, 468 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/cli/main.py; 67 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/cli/main_parser.py; 109, 110 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/commands/completion.py; 118 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/commands/freeze.py; 107

	Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/utils/entrypoints.py; 35 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 1705, 1707, 1724 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/pyparsing/core.py; 5911, 5917 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/rich/style.py; 730 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/dist.py; 252 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/text_file.py; 153 Runner/RobilityRunner/Python/Lib/site-packages/wheel/macosx_libfile.py; 412 RobilityActivites/FlaUInspect/Core/ElementHighlighter.cs; 30 RobilityActivites/Robility.Cognitive/Canvas.cs; 177 RobilityActivites/Robility.ExcelAutomationV1/Utilities/ClsClosedXmlExcelWrite.cs; 77, 79, 176, 182, 185, 198, 201, 208, 224, 235, 252, 259, 261, 276, 280, 283, 296, 300, 303, 314, 320, 323, 357, 369, 370, 374, 429, 431, 432, 434 RobilityActivites/Robility.GenAI.Test/BusinessLayer/ContentGenerationExecutionTests.cs; 89, 187, 286 RobilityActivites/Robility.GenAI.Test/BusinessLayer/PiiFilteringExecutionTests.cs; 65, 156 RobilityActivites/Robility.GenAI.Test/DetectLanguageTest.cs; 61, 148 RobilityActivites/Robility.GenAI.Test/NamedEntityRecognitionTests.cs; 108, 209 RobilityActivites/Robility.GenAI.Test/SummarizeTextTest.cs; 85, 164 RobilityActivites/Robility.MarkplacePythonExecution/MainWindow.xaml.cs; 65 RobilityActivites/Robility.MicrosoftOutlook365/GetMaillistOffice365.cs; 152 RobilityActivites/Robility.WebAutomation/AttachToBrowser.cs; 247 RobilityActivites/Robility.WebAutomation_V3/AttachToBrowser.cs; 247 RobilityActivites/RobilityAzureServicesExecution/NamedPipe/NamedPipeServer.cs; 65 RobilityActivites/RobilityVideoRecorder/NamedPipe/NamedPipeClient.cs; 42 RobilityActivites/UIExplore/UIExplore/Views/MainWindow.xaml.cs; 1523
Observation	During assessment it was observed that using WriteLine() rather than a dedicated logging facility makes it difficult to monitor the program behaviour.
Severity Rating	Low
Impact	The problem is that writing directly to standard output or standard error is often used as an unstructured form of logging. Structured logging facilities provide features like logging levels, uniform formatting, a logger identifier, timestamps, and, perhaps most critically, the ability to direct the log messages to the right place. When the use of system output streams is jumbled together with the code that uses loggers properly, the result is often a well-kept log that is missing critical information.
Recommendation	It is recommended to use a .NET logging facility rather than Console.WriteLine.
References	https://vulncat.fortify.com/en/detail?category=Poor+Logging+Practice&subcategory=Use+of+a+System+Output+Stream

Proof of Concept:

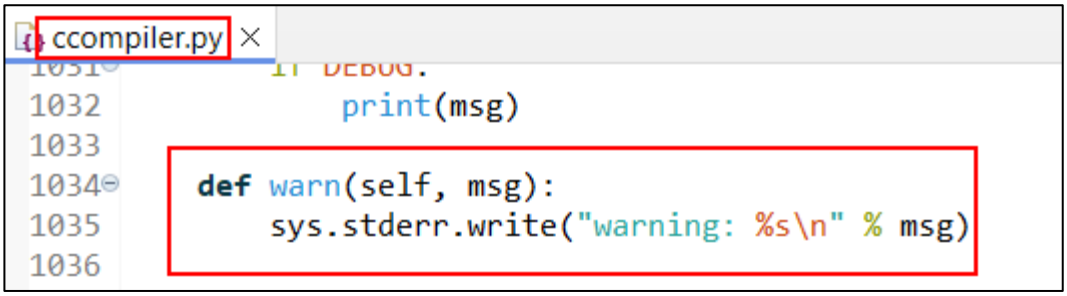


FIGURE 38: POOR LOGGING PRACTICE: USE OF A SYSTEM OUTPUT STREAM

39. RESOURCE INJECTION	
Source File	RobilityActivites/Robility.OutlookAutomation/Forward.cs; 174 RobilityActivites/Robility.OutlookAutomation/NewMail.cs; 126 RobilityActivites/Robility.OutlookAutomation/Reply.cs; 161 RobilityActivites/Robility.SalesForce/InsertRecord.cs; 137
Observation	During assessment it was observed that attackers are able to control the resource identifier argument, which could enable them to access or modify otherwise protected system resources.
Severity Rating	Low
Impact	A resource injection issue occurs when the following two conditions are met: • An attacker is able to specify the identifier used to access a system resource. • By specifying the resource, the attacker gains a capability that would not otherwise be permitted.
Recommendation	It is recommended to use a level of indirection: create a list of legitimate resource names that a user is allowed to specify, and only allow the user to select from the list. With this approach the input provided by the user is never used directly to specify the resource name.
References	https://vulncat.fortify.com/en/detail?category=Resource+Injection

Proof of Concept:

Forward.cs

```
170                 }
171                 newmail = mailItemf;
172             }
173             newmailf = mailItem.Forward();
174             newmail.Body += newmailf.Body;
175             newmail.Subject = mailItem.Subject;
176
```

FIGURE 39: RESOURCE INJECTION

40. SETTING MANIPULATION	
Source File	RobilityDesigner/RunnerInstance/WorkflowExecution/Runner.cs; 1460
Observation	During assessment it was observed that an attacker is able to control one of the arguments which can lead to a disruption of service or unexpected application behavior.
Severity Rating	Low
Impact	Setting manipulation vulnerabilities occur when an attacker can control values that govern the behavior of the system, manage specific resources, or in some way affect the functionality of the application.
Recommendation	It is recommended to not allow untrusted data to control sensitive values. In many cases where this error occurs, the application expects a particular input to hold only a very small range of values.
References	https://vulncat.fortify.com/en/detail?category=Setting+Manipulation

Proof of Concept:

Runner.cs

```
1458
1459            var existing = Console.Out;
1460            Console.SetOut(
1461                new TeeTextWriter(existing, _trayLogForwarder));
1462        }
1463    }
1464
```

FIGURE 40: SETTING MANIPULATION

41. SYSTEM INFORMATION LEAK	
Source File	RobilityDesigner/Functions/ExecuteXamlWorkflow/ClsTemplateService.cs; 81 RobilityDesigner/Functions/ExecuteXamlWorkflow/Connect.cs; 124 RobilityDesigner/Functions/ExecuteXamlWorkflow/InvokeDll.cs; 99, 135 RobilityDesigner/Functions/ExecuteXamlWorkflow/InvokeTemplate.cs; 139 RobilityDesigner/Functions/ExecuteXamlWorkflow/InvokeWorkflow.cs; 193 RobilityDesigner/Functions/SmartSpy/MainWindow.xaml.cs; 1663 RobilityDesigner/Robility.Launcher/ManageFeatures/Coreactivitymove.cs; 140 RobilityDesigner/Robility.Launcher/ViewModel/Connect.cs; 87 RobilityDesigner/ViewModel/Connect.cs; 182 Runner/SmartRPALogonService/LogonClass/RunLogon.cs; 413, 797 RobilityActivites/FlaUInspect/ViewModels/ElementViewModel.cs; 85 RobilityActivites/FlaUInspect/ViewModels/MainViewModel.cs; 556 RobilityActivites/ModernDesktopSpy/ViewModels/ElementViewModel.cs; 201 RobilityActivites/Robility.Cognitive/AbbyyCloudOCR.cs; 302, 312, 319, 338, 508, 579 RobilityActivites/Robility.Cognitive/Designer/dsAbbyyOCR.xaml.cs; 46, 94 RobilityActivites/Robility.Cognitive/Designer/dsActivityOcr.xaml.cs; 75 RobilityActivites/Robility.Cognitive/Designer/dsGoogleVisionOCR.xaml.cs; 76, 93, 118 RobilityActivites/Robility.Cognitive/Designer/dsImageEnhancement.xaml.cs; 77, 100 RobilityActivites/Robility.Cognitive/Designer/dsInvoiceReadDesigner.xaml.cs; 39 RobilityActivites/Robility.Cognitive/Designer/dsMicrosoftVisionOCR.xaml.cs; 41 RobilityActivites/Robility.Cognitive/Designer/dsPOReadDesigner.xaml.cs; 39 RobilityActivites/Robility.Cognitive/Designer/dsW9ReadDesigner.xaml.cs; 40 RobilityActivites/Robility.Cognitive/DetectLanguage.cs; 196 RobilityActivites/Robility.Cognitive/GoogleTextTranslator.cs; 118 RobilityActivites/Robility.Cognitive/GoogleVisionOCR.cs; 283 RobilityActivites/Robility.Cognitive/ImageCompression.cs; 35 RobilityActivites/Robility.Cognitive/ImageEnhancement.cs; 348 RobilityActivites/Robility.Cognitive/InvoiceRead.cs; 227 RobilityActivites/Robility.Cognitive/MicrosoftTranslator.cs; 149 RobilityActivites/Robility.Cognitive/MicrosoftVisionOCR.cs; 251 RobilityActivites/Robility.Cognitive/OCRTEXT.cs; 229 RobilityActivites/Robility.Cognitive/PORead.cs; 214 RobilityActivites/Robility.Cognitive/W9Read.cs; 217 RobilityActivites/Robility.CoreActivities.Tests/BusinessLayer/StartProcessHelperTest.cs; 159 RobilityActivites/Robility.DataTable/frmgridbox.cs; 122 RobilityActivites/Robility.DesktopAutomation/Automation/UIAutomation/Window.cs; 337, 342 RobilityActivites/Robility.DesktopAutomation/Dock.cs; 219 RobilityActivites/Robility.DesktopAutomation/Range.cs; 246

	RobilityActivites/Robility.DesktopAutomation/Scroll.cs; 278 RobilityActivites/Robility.DesktopAutomation/SecureTypeText.cs; 367 RobilityActivites/Robility.DesktopAutomation/Utilities/ElementExtraction.cs; 330 RobilityActivites/Robility.DesktopAutomation/View.cs; 222 RobilityActivites/Robility.DesktopAutomationUIA3/Automation/UIAutomation/Window.cs; 332, 337 RobilityActivites/Robility.DesktopAutomationUIA3/OpenSpyApplication.cs; 263 RobilityActivites/Robility.DesktopAutomation_Production/Automation/UIAutomation/Window.cs; 332, 337 RobilityActivites/Robility.DesktopAutomation_Production/Designer/DsDock.xaml.cs; 92, 203, 246, 281, 317, 388 RobilityActivites/Robility.DesktopAutomation_Production/Designer/DsRange.xaml.cs; 91, 250, 293, 362 RobilityActivites/Robility.DesktopAutomation_Production/Designer/DsScroll.xaml.cs; 90, 230, 296 RobilityActivites/Robility.DesktopAutomation_Production/Designer/DsSecureTypeText.xaml.cs; 111, 241, 288, 302 RobilityActivites/Robility.DesktopAutomation_Production/Designer/DsView.xaml.cs; 86, 227, 301 RobilityActivites/Robility.DictionaryAutomation/frmdictionviewer.cs; 154 RobilityActivites/Robility.ExcelAutomation/Common/UpdateAxisBoundsSupportClass.cs; 267, 282 RobilityActivites/Robility.ExcelAutomation/GetTableRange.cs; 207 RobilityActivites/Robility.ExcelAutomation/RefreshPivotTable.cs; 253 RobilityActivites/Robility.ExcelAutomation/UpdateChartChildMethodcs.cs; 155, 208, 225, 242, 256 RobilityActivites/Robility.ExcelAutomationV1/Utilities/ClsClosedXmlExcelWrite.cs; 54, 243, 287, 327, 381, 446 RobilityActivites/Robility.Generic/Designer/ParallelForEachDesigner.xaml.cs; 38 RobilityActivites/Robility.GoogleCognitiveServices/Designer/dsVisionOCR.xaml.cs; 39, 64 RobilityActivites/Robility.GoogleDrive/Common/FileSelect.cs; 216 RobilityActivites/Robility.GoogleDrive/Common/MovefilePartial.cs; 91 RobilityActivites/Robility.ImageAutomation/ImageFunction.cs; 225, 431 RobilityActivites/Robility.ImageAutomation/Utilities/Window.cs; 249, 254 RobilityActivites/Robility.Interact/Utility/Util.cs; 244 RobilityActivites/Robility.Invoke/ClsTemplateService.cs; 165 RobilityActivites/Robility.Invoke/Connect.cs; 124 RobilityActivites/Robility.Invoke/InvokeDll.cs; 93, 115 RobilityActivites/Robility.Invoke/InvokeTemplate.cs; 139 RobilityActivites/Robility.Invoke/InvokeWorkflow.cs; 187 RobilityActivites/Robility.Manager/ApiService.cs; 316, 422 RobilityActivites/Robility.Manager/SetAsset.cs; 165

	RobilityActivites/Robility.MicrosoftCognitiveServices/Designer/dsVisionOCR.xaml.cs ; 40, 65 RobilityActivites/Robility.MicrosoftEntityExtraction/Robility.MicrosoftEntityExtracti on/MicrosoftEntityExtraction.cs; 153 RobilityActivites/Robility.MicrosoftEntityExtraction/SmartRPA.Activities.MicrosoftE ntityExtraction/MicrosoftEntityExtraction.cs; 158 RobilityActivites/Robility.MicrosoftOutlook365/GetMaillistOffice365.cs; 161 RobilityActivites/Robility.MouseAutomation/Window.cs; 179, 184 RobilityActivites/Robility.NLTKEntityextraction/NLTKNamedentityExtraction.cs; 163 RobilityActivites/Robility.PDFAutomation/BusinessLayer/MergeFileExecution.cs; 41 RobilityActivites/Robility.PDFAutomation/BusinessLayer/PdfCreateFunctionality.cs; 82, 106 RobilityActivites/Robility.PDFAutomation/BusinessLayer/PdfPageToImageExecute.c s; 50, 99 RobilityActivites/Robility.PDFAutomation/BusinessLayer/TextExtractorExecute.cs; 42 RobilityActivites/Robility.PDFAutomation/Validationclass.cs; 37, 54 RobilityActivites/Robility.Recorder/Designer/frmRecording.cs; 1196 RobilityActivites/Robility.SalesForceToken/ApiHelper.cs; 59 RobilityActivites/Robility.SmartInteract/AddTransaction.cs; 163 RobilityActivites/Robility.SmartInteract/CheckDuplicateTransaction.cs; 136 RobilityActivites/Robility.SmartInteract/ClearMasterData.cs; 129 RobilityActivites/Robility.SmartInteract/CompleteTransaction.cs; 161 RobilityActivites/Robility.SmartInteract/GetMasterData.cs; 139 RobilityActivites/Robility.SmartInteract/GetTransaction.cs; 184 RobilityActivites/Robility.SmartInteract/GetTransactionCount.cs; 167 RobilityActivites/Robility.SmartInteract/GetTransactionHistory.cs; 146 RobilityActivites/Robility.SmartInteract/SearchTransaction.cs; 153 RobilityActivites/Robility.SmartInteract/UpdateMasterData.cs; 156 RobilityActivites/Robility.WebAutomation/AttachToBrowser.cs; 109, 115, 184, 209 RobilityActivites/Robility.WebAutomation/Cursor/WindowHandle.cs; 305, 310 RobilityActivites/Robility.WebAutomation/Designer/dsAttachToBrowser.xaml.cs; 42 RobilityActivites/Robility.WebAutomation/DisconnectBrowser.cs; 129, 220 RobilityActivites/Robility.WebAutomation/SecureSetText.cs; 275, 1158 RobilityActivites/Robility.WebAutomation/SwitchAlert.cs; 127, 210, 227, 312 RobilityActivites/Robility.WebAutomation/SwitchToFrame.cs; 175, 300, 406 RobilityActivites/Robility.WebAutomation/SwitchToWindow.cs; 143, 210, 280 RobilityActivites/Robility.WebAutomation_V3/AttachToBrowser.cs; 109, 115, 184, 209 RobilityActivites/Robility.WebAutomation_V3/Cursor/WindowHandle.cs; 312, 317 RobilityActivites/Robility.WebAutomation_V3/Designer/dsAttachToBrowser.xaml.cs ; 42 RobilityActivites/Robility.WebAutomation_V3/DisconnectBrowser.cs; 129, 220 RobilityActivites/Robility.WebAutomation_V3/InjectJS.cs; 196, 212

	RobilityActivites/Robility.WebAutomation_V3/SwitchAlert.cs; 127, 210, 227, 312 RobilityActivites/Robility.WebAutomation_V3/SwitchToFrame.cs; 175, 300, 406 RobilityActivites/Robility.WebAutomation_V3/SwitchToWindow.cs; 143, 210, 280 RobilityActivites/Robility.WebAutomation_V3/Utility/Utils.cs; 576, 581 RobilityActivites/RobilityAzureServicesExecution/Program.cs; 29 RobilityActivites/RobilityWebClient/Designer/DesignerREST.xaml.cs; 274, 316 RobilityActivites/RobilityWebClient/Designer/DesignerSoapClientPartial.cs; 136
Observation	During assessment it was observed that the mentioned function reveals system data or debugging information. The information revealed by WriteLine() could help an adversary form a plan of attack.
Severity Rating	Low
Impact	An information leak occurs when system data or debug information leaves the program through an output stream or logging function.
Recommendation	It is recommended to write error messages with security in mind. In production environments, turn off detailed error information in favour of brief messages.
References	https://vulncat.fortify.com/en/detail?category=System+Information+Leak

Proof of Concept:

RunLogon.cs

```
408
409         private XmlDocument LoadTemplateDocument(string templatePath)
410         {
411             if (!File.Exists(templatePath))
412             {
413                 throw new FileNotFoundException($"Template file not found at: {templatePath}");
414             }
415
```

FIGURE 41: SYSTEM INFORMATION LEAK

42. SYSTEM INFORMATION LEAK: INTERNAL	
Source File	RobilityDesigner/Execution/WorkflowDebugger.cs; 100 RobilityDesigner/Execution/WorkflowDebuggerBase.cs; 143 RobilityDesigner/Execution/WorkflowRunner.cs; 137 RobilityDesigner/Execution/WorkflowServiceHostDebugger.cs; 56 RobilityDesigner/Execution/WorkflowServiceHostRunner.cs; 83 RobilityDesigner/Python/Lib/site-packages/PIL/features.py; 246, 248, 251, 255 RobilityDesigner/Python/Lib/site-packages/_distutils_hack/__init__.py; 64 RobilityDesigner/Python/Lib/site-packages/pip/_internal/cli/autocompletion.py; 67, 98, 115 RobilityDesigner/Python/Lib/site-packages/pip/_internal/cli/parser.py; 175 RobilityDesigner/Python/Lib/site-packages/pip/_internal/operations/install/wheel.py; 109 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 557 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/packaging/_musllinux.py; 132, 136 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/pygments/cmdline.py; 289, 331, 337, 354, 370, 373, 400, 425, 431, 439, 444 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/rich/pretty.py; 994 RobilityDesigner/Python/Lib/site-packages/pkg_resources/_vendor/packaging/_musllinux.py; 76, 80 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/bcppcompiler.py; 398 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/ccompiler.py; 1032 RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/dist.py; 728 RobilityDesigner/Python/Lib/site-packages/setuptools/_vendor/packaging/_musllinux.py; 76, 80 RobilityDesigner/Python/Lib/site-packages/wheel/bdist_wheel.py; 334 RobilityDesigner/Python/Lib/site-packages/wheel/cli/__init__.py; 153 RobilityDesigner/Python/Lib/site-packages/wheel/cli/pack.py; 70 RobilityDesigner/Python/Lib/site-packages/wheel/macosx_libfile.py; 413 RobilityDesigner/Python/Lib/site-packages/wheel/vendored/packaging/_musllinux.py; 76, 80 RobilityDesigner/Python/get-pip.py; 33 RobilityDesigner/RunnerInstance/Utilities/ActivityTrayBridge.cs; 185 RobilityDesigner/UIExplore/SpyClass/Log.cs; 39 Runner/ProductUpdater/App.xaml.cs; 91 Runner/RobilityRunner/App.xaml.cs; 319 Runner/RobilityRunner/Python/Lib/site-packages/PIL/features.py; 246, 248, 251, 255 Runner/RobilityRunner/Python/Lib/site-packages/_distutils_hack/__init__.py; 64

	Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/cli/autocompletion.py; 67, 98, 115 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/cli/main.py; 66 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/cli/parser.py; 175 Runner/RobilityRunner/Python/Lib/site-packages/pip/_internal/operations/install/wheel.py; 109 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/distlib/util.py; 557 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/packaging/_musllinux.py; 132, 136 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/pygments/cmdline.py; 289, 331, 337, 354, 370, 373, 400, 425, 431, 439, 444 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/pyparsing/core.py; 5915 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/rich/pretty.py; 994 Runner/RobilityRunner/Python/Lib/site-packages/pkg_resources/_vendor/packaging/_musllinux.py; 76, 80 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/bcppcompiler.py; 398 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/ccompiler.py; 1032, 1035 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/core.py; 206 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/dist.py; 728 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_vendor/packaging/_musllinux.py; 76, 80 Runner/RobilityRunner/Python/Lib/site-packages/wheel/bdist_wheel.py; 334 Runner/RobilityRunner/Python/Lib/site-packages/wheel/cli/__init__.py; 153 Runner/RobilityRunner/Python/Lib/site-packages/wheel/cli/pack.py; 70 Runner/RobilityRunner/Python/Lib/site-packages/wheel/macosx_libfile.py; 413, 468 Runner/RobilityRunner/Python/Lib/site-packages/wheel/vendored/packaging/_musllinux.py; 76, 80 Runner/RobilityRunner/Python/get-pip.py; 33 Runner/WPFNamePipeListner/MainWindow.xaml.cs; 68 RobilityActivites/Robility.Cognitive/GoogleAnnotate.cs; 39 RobilityActivites/Robility.Cognitive/ImageOptimization.cs; 49 RobilityActivites/Robility.GoogleCognitiveServices/VisionOCR.cs; 638 RobilityActivites/UIExplore/SpyClass/Log.cs; 39 RobilityActivites/UIExplore/UIExplore/Helper/Connect.cs; 55 RobilityActivites/UIExplore/UIExplore/SpyClass/Log.cs; 36
Observation	During assessment it was observed that the mentioned function reveals system data or debugging information. The information revealed by Write() could help an adversary form a plan of attack.

Severity Rating	Low
Impact	An internal information leak occurs when system data or debug information is sent to a local file, console, or screen via printing or logging.
Recommendation	It is recommended to write error messages with security in mind. In production environments, turn off detailed error information in favour of brief messages. Restrict the generation and storage of detailed output that can help administrators and programmers diagnose problems.
References	https://vulncat.fortify.com/en/detail?category=System+Information+Leak&subcategory=Internal

Proof of Concept:

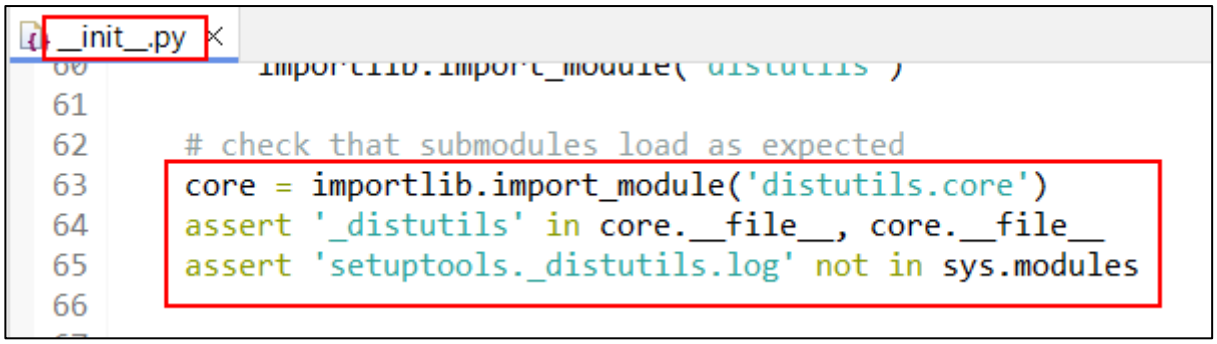


FIGURE 42: SYSTEM INFORMATION LEAK: INTERNAL

43. UNCHECKED RETURN VALUE	
Source File	RobilityDesigner/Functions/RobilityChromeNativeApp/Program.cs; 154, 160 RobilityDesigner/Functions/RobilityEdgeNativeApp/Program.cs; 151, 157
Observation	During assessment it was observed that the mentioned method ignores the value returned by Read(), which could cause the program to overlook unexpected states and conditions.
Severity Rating	Low
Impact	This behavior makes it important for programmers to examine the return value from Read() and other IO methods and ensure that they receive the amount of data they expect.
Recommendation	It is recommended to loop or check until you securely capture all 4 required bytes.
References	https://vulncat.fortify.com/en/detail?category=Unchecked+Return+Value

Proof of Concept:

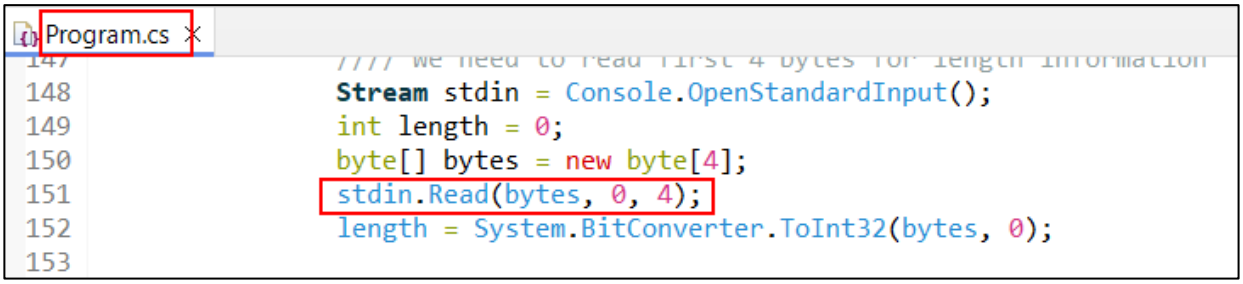


FIGURE 43: UNCHECKED RETURN VALUE

44. UNSAFE NATIVE INVOKE	
Source File	RobilityDesigner/Functions/SmartRPAActivities/RobotFunctions.cs; 520 RobilityActivites/JavaElementExtractor/Core/GobalHook.cs; 68, 69, 75, 76 RobilityActivites/Robility.FSAutomation/Beep.cs; 96 RobilityActivites/Robility.InternetExplorer/Utilities/MouseHoverRuntime.cs; 31 RobilityActivites/Robility.InternetExplorer_Production/MouseHover.cs; 360 RobilityActivites/Robility.UIVision/ClickHelper.cs; 152 RobilityActivites/Robility.UIVision/Common/Helper/WindowHelper.cs; 102 RobilityActivites/Robility.UIVision/HoverHelper.cs; 90 RobilityActivites/Robility.UIVision/TypeIntoHelper.cs; 96, 127, 130
Observation	During assessment it was observed that the mentioned method is a Platform Invocation Services or P/Invoke call. Improper use of P/Invoke can render managed applications vulnerable to security flaws in other languages.
Severity Rating	Low
Impact	Unsafe Native Invoke errors occur when a managed application uses P/Invoke to call native (unmanaged) code written in another programming language.
Recommendation	It is recommended to audit all source code comprising a given application, including native methods implemented in native code.
References	http://msdn.microsoft.com/en-us/library/55d3thsc.aspx

Proof of Concept:

Beep.cs

```
92
93                  ChkDuration(Intduration);
94                  ChkVolume(IntVolume);
95
96                  FSAutomationCommon.Beep(IntVolume, Intduration);
97
98                  Result.Set(context, true);
99                  logger.Trace(string.Format(Clsutility.cultureInfo, rm.GetString("Successmsg"),
100                             processName, DisplayName), CultureInfo.InvariantCulture);
```

FIGURE 44: UNSAFE NATIVE INVOKE

45. UNSAFE REFLECTION	
Source File	RobilityDesigner/Python/Lib/site-packages/setuptools/_distutils/dist.py; 828 RobilityDesigner/ReusableObjects/ViewModel/ReusableObjectViewModel.cs; 693, 879 RobilityDesigner/ViewModel/ImportWorkflow/ImportWorkflows.cs; 125 RobilityDesigner/ViewModel/MainWindwoActiproViewModel.cs; 2043, 2046, 2066, 4516 RobilityDesigner/ViewModel/PublishProjectDetails.cs; 81, 123 RobilityDesigner/ViewModel/SaveWorkflows.cs; 103, 314 Runner/RobilityRunner/Python/Lib/site-packages/setuptools/_distutils/dist.py; 828
Observation	During assessment it was observed that the attackers are able to control an argument to the reflection method, which could allow them to create unexpected control flow paths through the application, potentially bypassing security checks.
Severity Rating	Low
Impact	If an attacker can supply values that the application then uses to determine which class to instantiate or which method to invoke, the potential exists for the attacker to create control flow paths through the application that were not intended by the application developers.
Recommendation	It is recommended to create a list of legitimate names that users are allowed to specify, and only allow users to select from the list. With this approach, input provided by users is never used directly to specify a name that is passed to the reflection API.
References	https://vulncat.fortify.com/en/detail?category=Unsafe+Reflection

Proof of Concept:

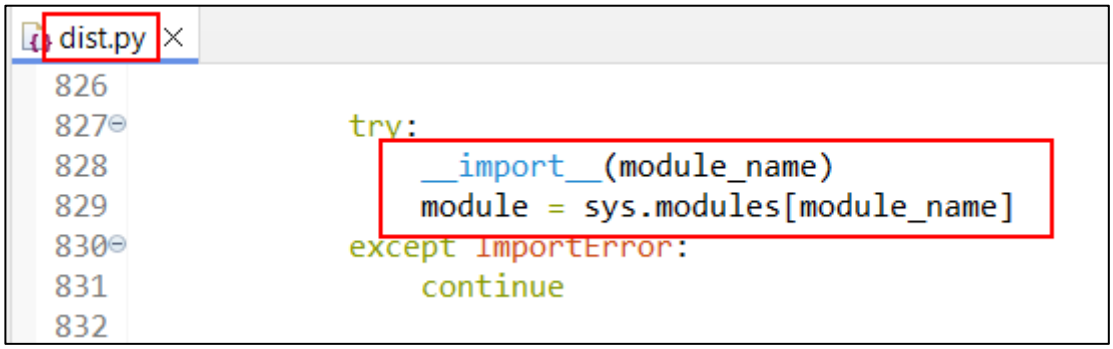


FIGURE 45: UNSAFE REFLECTION

46. WCF MISCONFIGURATION: THROTTLING NOT ENABLED	
Source File	Runner/ProductUpdateDownloader/App.config; 70 Runner/RobilityAssistedRobot/App.config; 73 Runner/ProductUpdater/App.config; 73 Runner/RunnerInstance/App.config; 75 Runner/RobilityRunner/App.config; 91
Observation	During assessment it was observed that the application uses a WCF endpoint with throttling not enabled.
Severity Rating	Low
Impact	Not placing a limit on the use of system resources could result in resource exhaustion and ultimately a denial of service.
Recommendation	It is recommended to enable WCF's service throttling feature and set limits appropriate for your application.
References	http://msdn.microsoft.com/en-us/library/ms731379.aspx

Proof of Concept:

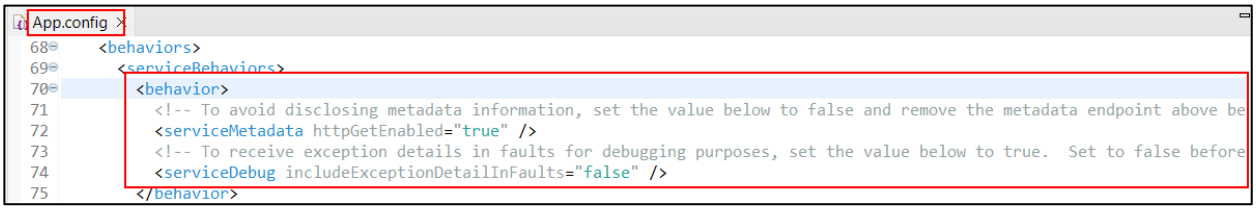


FIGURE 46: WCF MISCONFIGURATION: THROTTLING NOT ENABLED

47. WEAK CRYPTOGRAPHIC HASH	
Source File	RobilityDesigner/CoreActivities/Features/Robility.CoreActivities/1.1.9/System.Reflection.Metadata.xml; 7416 RobilityDesigner/Functions/FeatureManager/Features.cs; 126 RobilityDesigner/Functions/SmartRPAActivities/StringCipher.cs; 33, 75 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/distlib/database.py; 1024 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/distlib/index.py; 268 RobilityDesigner/Python/Lib/site-packages/pip/_vendor/requests/auth.py; 148, 156, 205 RobilityDesigner/Robility.Launcher/Utilities/StringCipher.cs; 32, 74 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/distlib/database.py; 1024 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/distlib/index.py; 268 Runner/RobilityRunner/Python/Lib/site-packages/pip/_vendor/requests/auth.py; 148, 156, 205 RobilityActivites/Robility.CryptographyAutomation/HashUtility.cs; 47, 49, 57
Observation	During assessment it was observed that weak cryptographic hashes cannot guarantee data integrity and should not be used in security-critical contexts.
Severity Rating	Low
Impact	Effective techniques for breaking MD and RIPEMD hashes are widely available, so those algorithms should not be relied upon for security. In the case of SHA-1, current techniques still require a significant amount of computational power and are more difficult to implement. However, attackers have found the Achilles' heel for the algorithm, and techniques for breaking it will likely lead to the discovery of even faster attacks.
Recommendation	It is recommended to discontinue the use of MD2, MD4, MD5, RIPEMD-160, and SHA-1 for data-verification in security-critical contexts. Currently, SHA-224, SHA-256, SHA-384, SHA-512, and SHA-3 are good alternatives. However, these variants of the Secure Hash Algorithm have not been scrutinized as closely as SHA-1, so be mindful of future research that might impact the security of these algorithms.
References	https://resources.bishopfox.com/resources/tools/other-free-tools/md4md5-collision-code/

Proof of Concept:

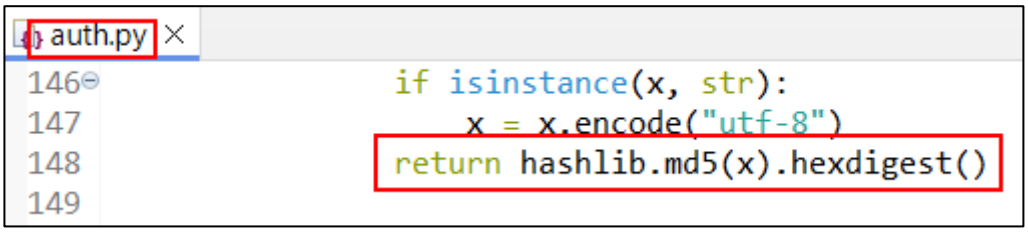


FIGURE 47: WEAK CRYPTOGRAPHIC HASH

48. WEAK CRYPTOGRAPHIC HASH: INSECURE PBE ITERATION COUNT	
Source File	RobilityDesigner/Functions/Robility.ServiceCall/TokenManager.cs; 247 RobilityDesigner/WorkflowServices/Service References/WorkflowServiceClient/Reference.cs; 1911 RobilityDesigner/WorkflowServices_Live/Service References/WorkflowServiceClient/Reference.cs; 1911 Runner/CommonHelper/ApplicationPath.cs; 140 Runner/ProductUpdateDownloader/ProductUpdater.cs; 243 Runner/Robility.ServiceCalls/TokenManager.cs; 256 Runner/RobilityRunner/RobilityClass/StringCipher.cs; 33, 75, 114, 160 Runner/RobilityServiceLayer/Service References/CredentialService/Reference.cs; 940 Runner/RobilityServiceLayer/Service References/DesignerService/Reference.cs; 2862 Runner/RobilityServiceLayer/Service References/FeatureService/Reference.cs; 227 Runner/RobilityServiceLayer/Service References/RunnerService/Reference.cs; 453 Runner/RobilityServiceLayer/Service References/TemplateRepository/Reference.cs; 2667 Runner/SmartRPALogonService/RobilityClass/StringCipher.cs; 33, 75, 106, 135 Runner/SmartRPALogonService/Service References/LogonService/Reference.cs; 391 Runner/SmartRPALogonService/Service References/WebService/Reference.cs; 237 RobilityActivites/Robility.AppIntegration/Common/EncryptInformation.cs; 34 RobilityActivites/Robility.CopilotControl/Common/EncryptInformation.cs; 35 RobilityActivites/Robility.ExcelAutomation/Common/EncryptionService.cs; 42, 80 RobilityActivites/Robility.GoogleDrive/Common/EncryptInformation.cs; 34 RobilityActivites/Robility.GoogleSheet/Robility.GoogleSheet/Common/EncryptInformation.cs; 34 RobilityActivites/Robility.Interact/Utility/EncryptInformation.cs; 30 RobilityActivites/Robility.Manager/ApiService.cs; 309, 348 RobilityActivites/Robility.Manager/CryptoHelper.cs; 35, 71 RobilityActivites/Robility.SmartInteract/ApplicationPath.cs; 130 RobilityActivites/Robility.Twilio/Common/EncryptInformation.cs; 36 RobilityActivites/Robility.ZenDesk/Common/EncryptInformation.cs; 34
Observation	During assessment it was observed that the iteration count used by a password-based key derivation function is too low.
Severity Rating	Low
Impact	A key derivation function is used to derive a key from a base key and other parameters. In a password-based key derivation function, the base key is a password and the other parameters are a salt value and an iteration count. An iteration count has traditionally served the purpose of increasing the cost of generating keys from a password. If the iteration count is too low, the feasibility of an attack increases as an attacker can compute "rainbow tables" for the application and more easily reverse hashed password values.

Recommendation	It is recommended that when using password-based key derivation functions, the iteration count should be at least 1000, but ideally 100,000 or greater.
References	https://www.ietf.org/rfc/rfc2898.txt

Proof of Concept:

ApplicationPath.cs

```
138             using (Aes encryptor = Aes.Create())
139             {
140                 Rfc2898DeriveBytes pdb = new Rfc2898DeriveBytes(encryptionKey, PredictableSalt());
141                 encryptor.Key = pdb.GetBytes(thirtyTwo);
142                 encryptor.IV = pdb.GetBytes(sixteen);
```

FIGURE 48: WEAK CRYPTOGRAPHIC HASH: INSECURE PBE ITERATION COUNT

49. WEAK CRYPTOGRAPHIC HASH: USER-CONTROLLED PBE SALT	
Source File	Functions/SmartRPAActivities/StringCipher.cs; 75
Observation	During assessment it was observed that the mentioned function includes user input within the salt value used within a Password-Based Key Derivation Function
Severity Rating	Low
Impact	This may enable the attacker to specify an empty salt, allowing for both more easily determined hashed values and a leak of information about how the program performs its cryptographic hashing.
Recommendation	It is recommended that the salt should never be user-controlled, even partially, nor hardcoded.
References	https://vulncat.fortify.com/en/detail?category=Weak+Cryptographic+Hash&subcategory=User-Controlled+PBE+Salt

Proof of Concept:

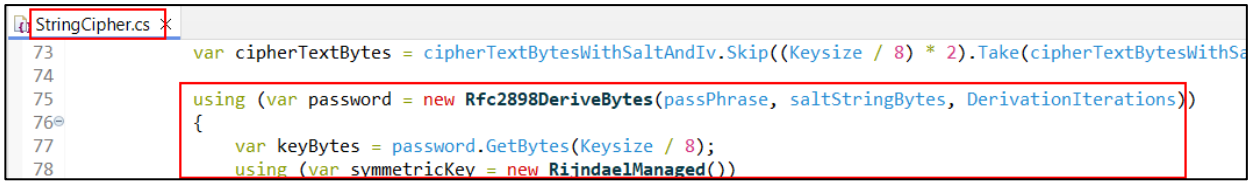


FIGURE 49: WEAK CRYPTOGRAPHIC HASH: USER-CONTROLLED PBE SALT

50. WEAK XML SCHEMA: TYPE ANY	
Source File	RobilityDesigner/WorkflowServices/Service References/WorkflowServiceClient/SmartRPAService.xsd; 25, 51, 77, 121, 147, 173, 199, 225, 251, 305, 331 RobilityDesigner/WorkflowServices/Service References/WorkflowServiceClient/SmartRPAService2.xsd; 12 RobilityDesigner/WorkflowServices_Live/Service References/WorkflowServiceClient/SmartRPAService.xsd; 25, 51, 77, 121, 147, 173, 199, 225, 251, 305, 331 RobilityDesigner/WorkflowServices_Live/Service References/WorkflowServiceClient/SmartRPAService2.xsd; 12 Runner/RobilityServiceLayer/Service References/DesignerService/DesignerService41.xsd; 25, 51, 77, 109, 137, 166, 192, 218, 244, 270, 296, 322, 376, 402, 429, 457, 501, 543, 572, 600, 630, 659 Runner/RobilityServiceLayer/Service References/DesignerService/DesignerService43.xsd; 12 Runner/RobilityServiceLayer/Service References/DesignerService/SmartRPAService42.xsd; 25, 51, 77, 107, 135, 161, 187, 213, 239, 265, 319, 345 Runner/RobilityServiceLayer/Service References/DesignerService/SmartRPAService43.xsd; 12 Runner/RobilityServiceLayer/Service References/DesignerService/service.xsd; 25, 51, 77, 108, 136, 165, 191, 217, 243, 269, 295, 321, 375, 401 Runner/RobilityServiceLayer/Service References/DesignerService/service2.xsd; 12 Runner/RobilityServiceLayer/Service References/DesignerService/service3.xsd; 25, 51, 77, 107, 135, 164, 190, 216, 242, 268, 294, 320, 374, 400 Runner/RobilityServiceLayer/Service References/DesignerService/service5.xsd; 12 Runner/RobilityServiceLayer/Service References/FeatureService/FeatureService4.xsd; 25, 51, 78, 106, 135, 194, 222 Runner/RobilityServiceLayer/Service References/FeatureService/FeatureService43.xsd; 12 Runner/RobilityServiceLayer/Service References/RunnerService/service.xsd; 25, 53, 79, 106, 133, 159, 186, 229, 256, 284 Runner/RobilityServiceLayer/Service References/RunnerService/service2.xsd; 12 Runner/RobilityServiceLayer/Service References/RunnerService/service3.xsd; 28, 57, 87, 115, 163, 192, 222, 252, 285, 312, 340 Runner/RobilityServiceLayer/Service References/RunnerService/service5.xsd; 12 Runner/SmartRPALogonService/Service References/LogonService/RunnerService42.xsd; 23, 50, 77, 103, 130, 172, 199 Runner/SmartRPALogonService/Service References/LogonService/RunnerService43.xsd; 12
Observation	During assessment it was observed that the type <any> element is being used.

Severity Rating	Low
Impact	The <any> element means arbitrary tags can be included in a valid document. Permitting arbitrary content makes it easier for attackers to perform attacks like XML injection.
Recommendation	It is recommended to explicitly define permissible elements instead of using the <any> element.
References	http://www.w3.org/TR/xmlschema-1/

Proof of Concept:

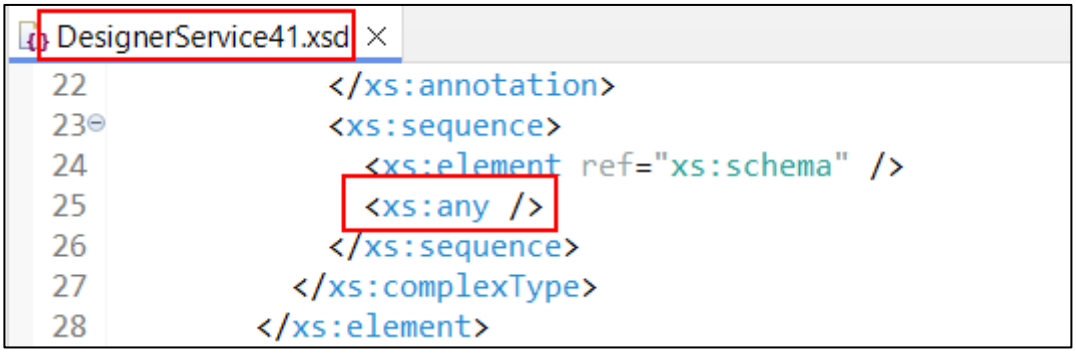


FIGURE 50: WEAK XML SCHEMA: TYPE ANY

51. WEAK XML SCHEMA: UNBOUNDED OCCURRENCES	
Source File	RobilityDesigner/Functions/RobilityUpdater/NLog.xsd; 5, 80, 94, 99, 121, 166, 248, 262, 263, 288, 351, 389, 439, 455, 640, 664, 675, 676, 765, 787, 835, 903, 915, 916, 918, 1003, 1007, 1032, 1092, 1130, 1156, 1243, 1269, 1569, 1596, 1681, 1713, 1720, 1768, 1798, 1976, 2008, 2012, 2041, 2145, 2161, 2322, 2354, 2380, 2474, 2477, 2499, 2517, 2537, 2563, 2595, 2615, 2635, 2667, 2669, 2683, 2785, 2786, 2792, 2797, 2801, 2870, 2894, 2895, 2955, 2997, 3023, 3031, 3074, 3088, 3098, 3100, 3180, 3208, 3212, 3213, 3300, 3329, 3361, 3393, 3425, 3457, 3531, 3538, 3545, 3552 RobilityDesigner/Functions/SmartRPAActivities/NLog.xsd; 5, 81, 95, 100, 122, 177, 253, 269, 283, 284, 309, 341, 361, 418, 613, 645, 689, 701, 702, 786, 808, 856, 914, 921, 925, 926, 928, 932, 1052, 1086, 1090, 1115, 1193, 1221, 1249, 1269, 1272, 1344, 1380, 1470, 1496, 1668, 1689, 1733, 1755, 1926, 1946, 2137, 2216, 2242, 2245, 2447, 2471, 2478, 2520, 2550, 2555, 2754, 2788, 2814, 2882, 2884, 2909, 2912, 2986, 3126, 3152, 3180, 3268, 3271, 3287, 3305, 3319, 3339, 3371, 3385, 3386, 3485, 3513, 3561, 3575, 3589, 3604, 3740, 3788, 3819, 3989, 4027, 4067, 4069, 4071, 4173, 4174, 4180, 4185, 4186, 4258, 4282, 4283, 4287, 4346, 4347, 4367, 4368, 4430, 4456, 4461, 4470, 4538, 4539, 4550, 4614, 4621, 4622, 4632, 4709, 4710, 4715, 4791, 4796, 4797, 4823, 4841, 4842, 4843, 4845, 4928, 4968, 4970, 4971, 4972, 5067, 5096, 5128, 5160, 5192, 5224, 5292, 5299, 5306, 5313 RobilityDesigner/NLog.xsd; 5, 81, 95, 100, 122, 177, 253, 269, 283, 284, 309, 341, 361, 418, 613, 645, 689, 701, 702, 786, 808, 856, 914, 921, 925, 926, 928, 932, 1052, 1086, 1090, 1115, 1193, 1221, 1249, 1269, 1272, 1344, 1380, 1470, 1496, 1668, 1689, 1733, 1755, 1926, 1946, 2137, 2216, 2242, 2245, 2447, 2471, 2478, 2520, 2550, 2555, 2754, 2788, 2814, 2882, 2884, 2909, 2912, 2986, 3126, 3152, 3180, 3268, 3271, 3287, 3305, 3319, 3339, 3371, 3385, 3386, 3485, 3513, 3561, 3575, 3589, 3604, 3740, 3788, 3819, 3989, 4027, 4067, 4069, 4071, 4173, 4174, 4180, 4185, 4186, 4258, 4282, 4283, 4287, 4346, 4347, 4367, 4368, 4430, 4456, 4461, 4470, 4538, 4539, 4550, 4614, 4621, 4622, 4632, 4709, 4710, 4715, 4791, 4796, 4797, 4823, 4841, 4842, 4843, 4845, 4928, 4968, 4970, 4971, 4972, 5067, 5096, 5128, 5160, 5192, 5224, 5292, 5299, 5306, 5313 RobilityDesigner/WorkflowServices/NLog.xsd; 5, 55, 69, 74, 96, 141, 210, 224, 225, 250, 276, 321, 335, 367, 383, 508, 526, 532, 533, 603, 625, 673, 723, 735, 736, 739, 817, 821, 846, 882, 914, 934, 1009, 1029, 1292, 1312, 1391, 1398, 1440, 1464, 1636, 1656, 1718, 1722, 1745, 1831, 1847, 1960, 1986, 2006, 2094, 2097, 2113, 2131, 2145, 2165, 2191, 2205, 2219, 2239, 2242, 2298, 2299, 2305, 2310, 2314, 2383, 2401, 2402, 2420, 2444, 2470, 2477, 2491, 2520, 2552, 2584, 2616, 2648, 2655, 2662, 2669 RobilityDesigner/WorkflowServices_Live/NLog.xsd; 5, 55, 69, 74, 96, 141, 210, 224, 225, 250, 276, 321, 335, 367, 383, 508, 526, 532, 533, 603, 625, 673, 723, 735, 736, 739, 817, 821, 846, 882, 914, 934, 1009, 1029, 1292, 1312, 1391, 1398, 1440, 1464, 1636, 1656, 1718, 1722, 1745, 1831, 1847, 1960, 1986, 2006, 2094, 2097, 2113, 2131, 2145, 2165, 2191, 2205, 2219, 2239, 2242, 2298, 2299, 2305, 2310, 2314,

	2383, 2401, 2402, 2420, 2444, 2470, 2477, 2491, 2520, 2552, 2584, 2616, 2648, 2655, 2662, 2669 Runner/RobilityRunner/NLog.xsd; 5, 80, 94, 99, 121, 166, 248, 262, 263, 288, 351, 389, 439, 455, 640, 664, 675, 676, 765, 787, 835, 903, 915, 916, 918, 1003, 1007, 1032, 1092, 1130, 1156, 1243, 1269, 1569, 1596, 1681, 1713, 1720, 1768, 1798, 1976, 2008, 2012, 2041, 2145, 2161, 2322, 2354, 2380, 2474, 2477, 2499, 2517, 2537, 2563, 2595, 2615, 2635, 2667, 2669, 2683, 2785, 2786, 2792, 2797, 2801, 2870, 2894, 2895, 2955, 2997, 3023, 3031, 3074, 3088, 3098, 3100, 3180, 3208, 3212, 3213, 3300, 3329, 3361, 3393, 3425, 3457, 3531, 3538, 3545, 3552 Runner/RobilityServiceLayer/Service References/FeatureService/FeatureService41.xsd; 5 Runner/RobilityServiceLayer/Service References/OCRService/Service11.xsd; 5 Runner/RobilityServiceLayer/Service References/TemplateRepository/FeatureService.xsd; 5, 48 Runner/RobilityServiceLayer/Service References/TemplateRepository/FeatureService3.xsd; 5, 42, 81, 140 Runner/RobilityServiceLayer/Service References/TemplateRepository/FeatureService4.xsd; 5 RobilityActivites/Robility.Cognitive/Service References/ServiceReference1/soap1.xsd; 107, 136, 163, 169, 222 RobilityActivites/Robility.Cognitive/Service References/ServiceReference1/soap2.xsd; 5, 11 RobilityActivites/Robility.SmartInteract/Service References/SmartInteract/Arrays.xsd; 5 RobilityActivites/Robility.SmartInteract/Service References/SmartInteract/service2.xsd; 24, 41, 59
Observation	During assessment it was observed that the unbounded occurrences is being used.
Severity Rating	Low
Impact	Setting a maxOccurs value to unbounded can lead to resources exhaustion and ultimately a denial of service.
Recommendation	It is recommended to limit maxOccurs to a reasonable number.
References	http://www.w3.org/TR/xmlschema-1/

Proof of Concept:

FeatureService.xsd

```
3   <xs:complexType name="ArrayOfUSP_Get_Compatible_Products_Result">
4     <xs:sequence>
5       <xs:element minOccurs="0" maxOccurs="unbounded" name="USP_Get_Compatible_Products_Result"
6     </xs:sequence>
7   </xs:complexType>
```

FIGURE 51: WEAK XML SCHEMA: UNBOUNDED OCCURRENCES

SOURCE COMPOSITION ANALYSIS

1. HEAP-BASED BUFFER OVERFLOW

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET.Core@3.0.0 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET and Magick.NET-Q16-x64 version.
Severity Rating	**Critical**
Impact	**CVE-2023-4863:** An attacker can craft a special WebP lossless file that triggers the ReadHuffmanCodes() function to allocate the HuffmanCode buffer with a size that comes from an array of precomputed sizes: kTableSize.
Recommendation	It is recommended to Upgrade Magick.NET.Core to version 13.3.0 or higher. Upgrade Magick.NET-Q16-x64 to version 14.14.0 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.10.4 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2023-5129

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 52: MAGICK.NET-Q16-X64 7.20.0.1

2. INTEGER OVERFLOW OR WRAPAROUND

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 version.
Severity Rating	**Critical**
Impact	**CVE-2026-23876:** ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-13 and 6.9.13-38, a heap buffer overflow vulnerability in the XBM image decoder (ReadXBMImage) allows an attacker to write controlled data past the allocated heap buffer when processing a maliciously crafted image file.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.2 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.10.3 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-23876

Proof of Concept:

packages.config

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <packages>
3    <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
4    <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
5    <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
6    <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
7    <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
8    <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
9    <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
10   <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
11   <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
12   <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
13   <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
14   <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
15   <package id="NLog" version="6.0.7" targetFramework="net481" />
16   <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
17   <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
18 </packages>
```

FIGURE 53: MAGICK.NET-Q16-X64 7.20.0.1

3. OUT-OF-BOUNDS WRITE

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 and Magick.NET-Q16-AnyCPU version.
Severity Rating	**Critical**
Impact	**CVE-2026-28693:** Affected versions of this package are vulnerable to Out-of-bounds Write or read, in ReadDIBImage() and WriteDIBImage() in the DIB coder, due to an integer overflow.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.4 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.10.4 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-28693

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 54: MAGICK.NET-Q16-X64 7.20.0.1

4. USE OF EXTERNALLY-CONTROLLED FORMAT STRING

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 and Magick.NET-Q16-AnyCPU version.
Severity Rating	**High**
Impact	**CVE-2025-55298** ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to ImageMagick versions 6.9.13-28 and 7.1.2-2, a format string bug vulnerability exists in InterpretImageFilename function where user input is directly passed to FormatLocaleString without proper sanitization.
Recommendation	It is recommended Upgrade Magick.NET-Q16-x64 to version 14.8.1 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.10.3 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2025-55298

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net401" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net401" />
  <package id="NLog" version="6.0.7" targetFramework="net401" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 55: MAGICK.NET-Q16-X64 7.20.0.1

5. RELEASE OF INVALID POINTER OR REFERENCE

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU and Magick.NET-Q16-x64 version.
Severity Rating	**High**
Impact	**CVE-2026-56364:** ImageMagick before 7.1.2-13 contains a memory leak vulnerability in LoadOpenCLDeviceBenchmark() function when parsing malformed OpenCL device profile XML files with unclosed device elements. Attackers with write access to the OpenCL cache directory can place malicious XML files to exhaust memory and cause denial of service.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-AnyCPU to version 14.10.2 or higher. Upgrade Magick.NET-Q16-x64 to version 14.10.2 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-56364

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 56: MAGICK.NET-Q16-X64 7.20.0.1

6. NULL POINTER DEREFERENCE

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU and Magick.NET-Q16-x64 version.
Severity Rating	**High**
Impact	**CVE-2026-23952:** Affected versions of this package are vulnerable to NULL Pointer Dereference via the MSL parser when processing a <comment> tag before any image is loaded. An attacker can cause a crash and denial of service by submitting a specially crafted MSL file that triggers a NULL pointer dereference during the handling of the comment tag
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.2 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.14.0 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-23952

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 57: MAGICK.NET-Q16-X64 7.20.0.1

7. STACK-BASED BUFFER OVERFLOW

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 version.
Severity Rating	**High**
Impact	**CVE-2026-30929** ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, MagnifyImage uses a fixed-size stack buffer. When using a specific image it is possible to overflow this buffer and corrupt the stack. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.13.0 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.10.3 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-30929

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net401" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net401" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 58: MAGICK.NET-Q16-X64 7.20.0.1

8. OFF-BY-ONE ERROR

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 and Magick.NET-Q16-AnyCPU version.
Severity Rating	**High**
Impact	**CVE-2026-25989** ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a crafted SVG file can cause a denial of service. An off-by-one boundary check (`>` instead of `>=`) that allows bypass the guard and reach an undefined `(size_t)` cast. Versions 7.1.2-15 and 6.9.13-40 contain a patch.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.3 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.13.1 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-25989

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 59: MAGICK.NET-Q16-X64 7.20.0.1

9. ALLOCATION OF RESOURCES WITHOUT LIMITS OR THROTTLING

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 and Magick.NET-Q16-AnyCPU version.
Severity Rating	**High**
Impact	**CVE-2026-24484** ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, Magick fails to check for multi-layer nested mvg conversions to svg, leading to DoS. Versions 7.1.2-15 and 6.9.13-40 contain a patch.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.3 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.13.1 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-24484

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net401" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net401" />
  <package id="NLog" version="6.0.7" targetFramework="net401" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 60: MAGICK.NET-Q16-X64 7.20.0.1

10. DIRECTORY TRAVERSAL	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 and Magick.NET-Q16-AnyCPU version.
Severity Rating	**High**
Impact	**CVE-2026-25965** ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, ImageMagick's path security policy is enforced on the raw filename string before the filesystem resolves it. As a result, a policy rule such as /etc/* can be bypassed by a path traversal.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.3 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.13.1 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-25965

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net401" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net401" />
  <package id="NLog" version="6.0.7" targetFramework="net401" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 61: MAGICK.NET-Q16-X64 7.20.0.1

11. TIME-OF-CHECK TIME-OF-USE (TOCTOU) RACE CONDITION	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 and Magick.NET-Q16-AnyCPU version.
Severity Rating	**High**
Impact	**CVE-2026-28689:** Affected versions of this package are vulnerable to Time-of-check Time-of-use (TOCTOU) Race Condition in the FileToBlobI() function, involving path policy enforcement. An attacker can perform a symlink swap after authorization on a domain="path" to bypass access restrictions.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.3 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.13.1 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-28689

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net401" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net401" />
  <package id="NLog" version="6.0.7" targetFramework="net401" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 62: MAGICK.NET-Q16-X64 7.20.0.1

12. ACCESS OF UNINITIALIZED POINTER	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 and Magick.NET-Q16-AnyCPU version.
Severity Rating	**High**
Impact	C**VE-2026-28691:** Affected versions of this package are vulnerable to Access of Uninitialized Pointer in ReadJBIGImage() in jbig.c.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.3 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.13.1 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-28691

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 63: MAGICK.NET-Q16-X64 7.20.0.1

13. UNCONTROLLED RECURSION	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 and Magick.NET-Q16-AnyCPU version.
Severity Rating	**High**
Impact	**CVE-2026-48734** ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-49 and 7.1.2-24, a crafted MVG file could result in a stack overflow due to a missing depth or visited-set check. This issue has been patched in versions 6.9.13-49 and 7.1.2-24.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.3 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.13.1 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-48734

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net401" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net401" />
  <package id="NLog" version="6.0.7" targetFramework="net401" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 64: MAGICK.NET-Q16-X64 7.20.0.1

14. USE AFTER FREE	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 and Magick.NET-Q16-AnyCPU version.
Severity Rating	**High**
Impact	**CVE-2026-53462** ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-50 and 7.1.2-25, when an allocation fails in CheckPrimitiveExtent this can result in a heap-use-after-free and result in a crash. This issue has been patched in versions 6.9.13-50 and 7.1.2-25.
Recommendation	It is recommended to Upgrade Magick.NET-Q16-x64 to version 14.10.3 or higher. Upgrade Magick.NET-Q16-AnyCPU to version 14.13.1 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-53462

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net401" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net401" />
  <package id="NLog" version="6.0.7" targetFramework="net401" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 65: MAGICK.NET-Q16-X64 7.20.0.1

15. DENIAL OF SERVICE (DOS)	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config : Robility.SmartRPACognitiveServices@0.0.0 and System.Net.Http@4.1.1 RobilityActivities\Robility.Cognitive/packages.config: Robility.Cognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.ExcelAutomationV1/packages.config: Robility.ExcelAutomationV1@0.0.0 and System.IO.Packaging@6.0.0 RobilityActivities\Robility.GoogleCognitive/packages.config: Robility.GoogleCognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.Interact/packages.config: Robility.Interact@0.0.0 and System.Net.Http@2.0.20126.16343
Observation	System.Net.Http is an Provides a programming interface for modern HTTP applications, including HTTP client components that allow applications to consume web services over HTTP and HTTP components that can be used by both clients and servers for parsing HTTP headers. Affected versions of this package are vulnerable to Denial of Service (DoS) as ASP.NET Core fails to properly validate web requests.
Severity Rating	**High**
Impact	A denial of service vulnerability exists when the ASP.NET Core fails to properly validate web requests. NOTE: Microsoft has not commented on third-party claims that the issue is that the TextEncoder.EncodeCore function in the System.Text.Encodings.Web package in ASP.NET Core Mvc before 1.0.4 and 1.1.x before 1.1.3 allows remote attackers to cause a denial of service by leveraging failure to properly calculate the length of 4-byte characters in the Unicode Non-Character range
Recommendation	It is recommended to Upgrade System.Net.Http to version 4.1.2, 4.3.2 or higher. Upgrade System.IO.Packaging to version 6.0.1, 8.0.1, 9.0.0-rc.2.24473.5 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2017-0247

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 66: SYSTEM.NET.HTTP 4.1.1

16. INFINITE LOOP	
Path	RobilityDesigner\Functions\SmartRPAActivities/packages.config:SmartRPAActivities @0.0.0 › System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/ChildSessionRunnerInstance\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\CommentOut\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ControlListView\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\DesignerDebugger\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ElementEditor\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ExecuteXamlWorkflow\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ExpressionEditorService\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\FeatureManager\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\GitLeaksScannerLib\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\InteractAPIClient\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ProductUpdateDownloader\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ProductUpdater\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ProjectSolution\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.App.Model\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.DebugTracking\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.Product.Update\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.RemoveUnused\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.ServiceCall\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.Utilities\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2

	RobilityDesigner/Functions\Robility.WorkflowAnalyzer\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\RobilityActivityTray\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\RobilityChromeNativeApp\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\RobilityEdgeNativeApp\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\RobilityUpdater\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\SmartRPAActivities\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\SmartSpy\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\TaskScheduler.Helper\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/ObjectRepository\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Robility.Launcher\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/RobilityRoboPoster\RobilityRoboPoster\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/RunnerInstance\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/UIExplore\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/WorkflowServices\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/WorkflowServices_Live\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityActivities\Robility.ExcelAutomation/packages.config: Robility.ExcelAutomation@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1 RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0 RobilityActivities\Robility.ExcelAutomation.Tests/packages.config: Robility.ExcelAutomation.Tests@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityActivities\Robility.FormBuilder/packages.config: Robility.FormBuilder@0.0.0 and System.Security.Cryptography.Xml@8.0.2
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU and Magick.NET-Q16-x64 version.

Severity Rating	**High**
Impact	**CVE-2026-40372:** Improper verification of cryptographic signature in ASP.NET Core allows an unauthorized attacker to elevate privileges over a network.
Recommendation	It is recommended to • Upgrade System.Security.Cryptography.Xml to version 8.0.3, 9.0.15, 10.0.7, 11.0.0-preview.3.26207.106 or higher • Upgrade Magick.NET-Q16-x64 to version 14.10.3 or higher. • Upgrade Magick.NET-Q16-AnyCPU to version 14.13.1 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-40372

Proof of Concept:

packages.config

```
<package id="System.Security.Cryptography.Pkcs" version="8.0.1" targetFramework="net481" />
<package id="System.Security.Cryptography.Primitives" version="4.3.0" targetFramework="net461" />
<package id="System.Security.Cryptography.X509Certificates" version="4.3.2" targetFramework="net461" />
<package id="System.Security.Cryptography.Xml" version="8.0.2" targetFramework="net481" />
<package id="System.Text.Encoding" version="4.3.0" targetFramework="net45" />
<package id="System.Text.Encoding.CodePages" version="10.0.3" targetFramework="net481" />
<package id="System.Text.Encoding.Extensions" version="4.3.0" targetFramework="net45" />
<package id="System.Text.RegularExpressions" version="4.3.1" targetFramework="net461" requireReinstallatio
```

FIGURE 67: SYSTEM.SECURITY.CRYPTOGRAPHY.XML 8.0.2

17. XML EXTERNAL ENTITY (XXE) INJECTION	
Path	RobilityDesigner\Functions\SmartRPAActivities/packages.config:SmartRPAActivities@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/ChildSessionRunnerInstance\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\CommentOut\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ControlListView\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\DesignerDebugger\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ElementEditor\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ExecuteXamlWorkflow\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ExpressionEditorService\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\FeatureManager\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\GitLeaksScannerLib\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\InteractAPIClient\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ProductUpdateDownloader\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ProductUpdater\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\ProjectSolution\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.App.Model\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.DebugTracking\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.Product.Update\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.RemoveUnused\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.ServiceCall\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\Robility.Utilities\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2

	RobilityDesigner/Functions\Robility.WorkflowAnalyzer\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\RobilityActivityTray\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\RobilityChromeNativeApp\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\RobilityEdgeNativeApp\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\RobilityUpdater\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\SmartRPAActivities\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\SmartSpy\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Functions\TaskScheduler.Helper\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/ObjectRepository\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/Robility.Launcher\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/RobilityRoboPoster\RobilityRoboPoster\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/RunnerInstance\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/UIExplore\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/WorkflowServices\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityDesigner/WorkflowServices_Live\packages.config: RobilityDesigner@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityActivities\Robility.ExcelAutomation/packages.config: Robility.ExcelAutomation@0.0.0 and System.Security.Cryptography.Xml@8.0.2 RobilityActivities\Robility.FormBuilder/packages.config: Robility.FormBuilder@0.0.0 and System.Security.Cryptography.Xml@8.0.2
Observation	During the assessment it was observed that the application is using vulnerable System.Security.Cryptography.Xml version.
Severity Rating	**High**
Impact	**CVE-2026-26171** Uncontrolled resource consumption in .NET allows an unauthorized attacker to deny service over a network.
Recommendation	It is recommended to • Upgrade System.Security.Cryptography.Xml to version 8.0.3, 9.0.15, 10.0.6, 11.0.0-preview.3.26207.106 or higher.

References	https://www.cve.org/CVERecord?id=CVE-2026-26171

Proof of Concept:

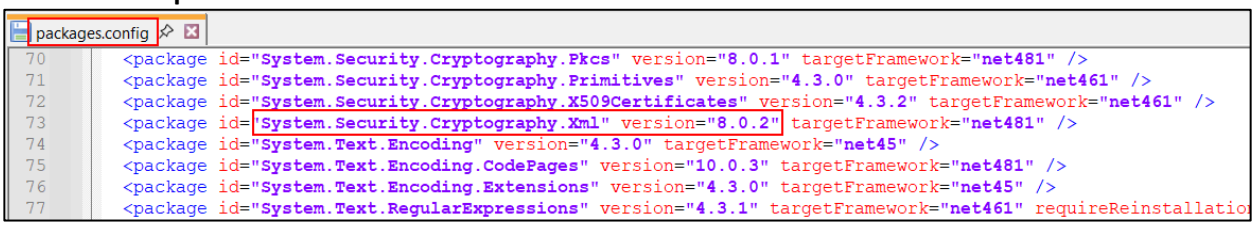


FIGURE 68: SYSTEM.SECURITY.CRYPTOGRAPHY.XML 8.0.2

18. INSECURE DEFAULTS	
Path	RobilityDesigner/WorkflowServices\packages.config: RobilityDesigner@0.0.0 and Newtonsoft.Json@9.0.1 RobilityDesigner\WorkflowServices/packages.config:WorkflowServices@0.0.0 and Newtonsoft.Json@9.0.1 RobilityActivities\Robility.AylienEntityExtraction/packages.config: Robility.AylienEntityExtraction@0.0.0 and Newtonsoft.Json@8.0.3 RobilityActivities\Robility.FacePlusPlus/packages.config: Robility.FacePlusPlus@0.0.0 and Newtonsoft.Json@9.0.1 RobilityActivities\Robility.MicrosoftEntityExtraction\SmartRPA.Activities.MicrosoftEntityExtraction/packages.config:SmartRPA.Activities.MicrosoftEntityExtraction@0.0.0 and Newtonsoft.Json@10.0.3 RobilityActivities\Robility.MicrosoftEntityExtraction\Robility.MicrosoftEntityExtraction/packages.config: Robility.MicrosoftEntityExtraction@0.0.0 and Newtonsoft.Json@10.0.3 RobilityActivities\Robility.Cognitive/packages.config : Robility.Cognitive@0.0.0 and Newtonsoft.Json@10.0.2 RobilityActivities\Robility.MicrosoftEntityExtraction\Robility.MicrosoftEntityExtraction/packages.config: Robility.MicrosoftEntityExtraction@0.0.0 and Newtonsoft.Json@10.0.3 WORKSPACE\SCR\Sutherland\Robility AI FPR\Source_Code\RobilityActivities\UIExplore\UIExplore/packages.config: UIExplore@0.0.0 and Newtonsoft.Json@12.0.1
Observation	During the assessment it was observed that the application is using vulnerable Newtonsoft.Json version.
Severity Rating	**High**
Impact	**CVE-2024-21907** Newtonsoft.Json before version 13.0.1 is affected by a mishandling of exceptional conditions vulnerability. Crafted data that is passed to the JsonConvert.DeserializeObject method may trigger a StackOverflow exception resulting in denial of service. Depending on the usage of the library, an unauthenticated and remote attacker may be able to cause the denial-of-service condition.
Recommendation	It is recommended to • Upgrade Newtonsoft.Json to version 13.0.1 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2024-21907
Proof of Concept:	

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Elasticsearch.Net" version="2.3.1" targetFramework="net45" />
  <package id="Newtonsoft.Json" version="9.0.1" targetFramework="net45" />
  <package id="NLog" version="4.3.10" targetFramework="net45" />
  <package id="NLog.Config" version="4.3.10" targetFramework="net45" />
  <package id="NLog.Schema" version="4.3.10" targetFramework="net45" />
  <package id="NLog.Targets.ElasticSearch" version="2.1.9" targetFramework="net45" />
</packages>
```

FIGURE 69: NEWTONSOFT.JSON 9.0.1

19. IMPROPER CERTIFICATE VALIDATION

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config : Robility.SmartRPACognitiveServices@0.0.0 and System.Net.Http@4.1.1 RobilityActivities\Robility.Cognitive/packages.config: Robility.Cognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.GoogleCognitive/packages.config: Robility.GoogleCognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.Interact/packages.config: Robility.Interact@0.0.0 and System.Net.Http@2.0.20126.16343
Observation	During the assessment it was observed that the application is using vulnerable System.Net.Http version.
Severity Rating	**High**
Impact	**CVE-2017-0248** Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7 allow an attacker to bypass Enhanced Security Usage taggings when they present a certificate that is invalid for a specific use, aka ".NET Security Feature Bypass Vulnerability."
Recommendation	It is recommended to • Upgrade System.Net.Http to version 4.1.2, 4.3.2 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2017-0248

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 70: SYSTEM.NET.HTTP 4.1.1

20. PRIVILEGE ESCALATION

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config : Robility.SmartRPACognitiveServices@0.0.0 and System.Net.Http@4.1.1 RobilityActivities\Robility.Cognitive/packages.config: Robility.Cognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.GoogleCognitive/packages.config: Robility.GoogleCognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.Interact/packages.config: Robility.Interact@0.0.0 and System.Net.Http@2.0.20126.16343
Observation	During the assessment it was observed that the application is using vulnerable System.Net.Http version.
Severity Rating	**High**
Impact	**CVE-2017-0249** An elevation of privilege vulnerability exists when the ASP.NET Core fails to properly sanitize web requests.
Recommendation	It is recommended to • Upgrade System.Net.Http to version 4.1.2, 4.3.2 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2017-0249

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 71: SYSTEM.NET.HTTP 4.1.1

21. INFORMATION EXPOSURE	
Path	RobilityActivities\Robility.Cognitive/packages.config: Robility.Cognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.GoogleCognitive/packages.config: Robility.GoogleCognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.Interact/packages.config: Robility.Interact@0.0.0 and System.Net.Http@2.0.20126.16343
Observation	During the assessment it was observed that the application is using vulnerable System.Net.Http version.
Severity Rating	**High**
Impact	**CVE-2018-8292** An information disclosure vulnerability exists in .NET Core when authentication information is inadvertently exposed in a redirect, aka ".NET Core Information Disclosure Vulnerability." This affects .NET Core 2.1, .NET Core 1.0, .NET Core 1.1, PowerShell Core 6.0.
Recommendation	It is recommended to • Upgrade System.Net.Http to version 2.0.20710, 4.0.1-beta-23225, 4.1.4, 4.3.4 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2018-8292

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 72: SYSTEM.NET.HTTP 4.1.1

22. OUT-OF-BOUNDS READ

Path	RobilityActivities\Robility.GoogleCognitive/packages.config: Robility.GoogleCognitive@0.0.0 and Microsoft.Bcl.Memory@10.0.3
Observation	During the assessment it was observed that the application is using vulnerable Microsoft.Bcl.Memory version.
Severity Rating	**High**
Impact	**CVE-2026-26127** Out-of-bounds read in .NET allows an unauthorized attacker to deny service over a network
Recommendation	It is recommended to Upgrade Microsoft.Bcl.Memory to version 9.0.14, 10.0.4 or higher.
References	https://www.cve.org/CVERecord?id=CVE-2026-26127

Proof of Concept:

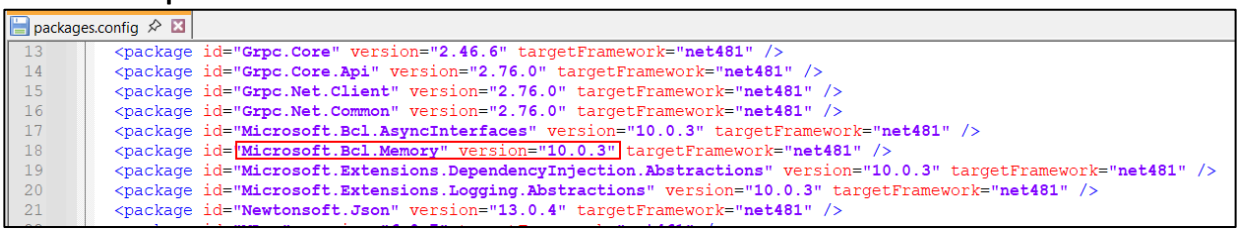


FIGURE 73: MICROSOFT.BCL.MEMORY 10.0.3

23. AUTHENTICATION BYPASS

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and System.Net.Http@4.1.1 RobilityActivities\Robility.Cognitive/packages.config: Robility.Cognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.GoogleCognitive/packages.config: Robility.GoogleCognitive@0.0.0 and System.Net.Http@4.3.1 RobilityActivities\Robility.Interact/packages.config: Robility.Interact@0.0.0 and System.Net.Http@2.0.20126.16343
Observation	During the assessment it was observed that the application is using vulnerable System.Net.Http version.
Severity Rating	**Medium**
Impact	**CVE-2018-8292:** An information disclosure vulnerability exists in .NET Core when authentication information is inadvertently exposed in a redirect, aka ".NET Core Information Disclosure Vulnerability." This affects .NET Core 2.1, .NET Core 1.0, .NET Core 1.1, PowerShell Core 6.0.
Recommendation	It is recommended to upgrade the System.Net.Http to the latest version 4.3.4.
References	https://nvd.nist.gov/vuln/detail/cve-2018-8292

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 74: SYSTEM.NET.HTTP 4.1.1

24. CRLF INJECTION	
Path	RobilityActivities\Robility.GmailAutomation/packages.config: Robility.GmailAutomation@0.0.0 and MimeKit@4.14.0
Observation	During the assessment it was observed that the application is using vulnerable MimeKit version.
Severity Rating	**Medium**
Impact	**CVE-2026-30227:** Affected versions of this package are vulnerable to CRLF Injection due to the InternetAddress not rejecting control characters. An attacker can inject SMTP commands by supplying a quoted local-part containing \r\n when constructing a MailboxAddress, causing the SMTP client to emit extra commands via MAIL FROM/RCPT TO.
Recommendation	It is recommended to upgrade the MimeKit to the latest version 4.15.1.
References	https://www.cve.org/CVERecord?id=CVE-2026-30227

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="AE.Net.Mail" version="1.7.10.0" targetFramework="net452" />
  <package id="BouncyCastle.Cryptography" version="2.6.1" targetFramework="net481" />
  <package id="Google.Apis" version="1.73.0" targetFramework="net481" />
  <package id="Google.Apis.Auth" version="1.73.0" targetFramework="net481" />
  <package id="Google.Apis.Core" version="1.73.0" targetFramework="net481" />
  <package id="Google.Apis.Gmail.v1" version="1.73.0.4029" targetFramework="net481" />
  <package id="MimeKit" version="4.14.0" targetFramework="net481" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net461" />
  <package id="Portable.BouncyCastle" version="1.9.0" targetFramework="net481" />
  <package id="System.Buffers" version="4.6.0" targetFramework="net481" />
  <package id="System.Memory" version="4.6.0" targetFramework="net481" />
  <package id="System.Numerics.Vectors" version="4.6.0" targetFramework="net481" />
  <package id="System.Runtime.CompilerServices.Unsafe" version="6.1.0" targetFramework="net481" />
</packages>
```

FIGURE 75: MIMEKIT 4.14.0.

25. RESOURCE INJECTION	
Path	RobilityActivities\Robility.FormBuilder/packages.config: Robility.FormBuilder@0.0.0 and NuGet.CommandLine@7.3.0 RobilityActivities\Robility.Notification/packages.config: Robility.Notification@0.0.0 and NuGet.CommandLine@7.3.0 RobilityActivities\Robility.Manager/packages.config: Robility.Manager@0.0.0 and NuGet.CommandLine@7.3.0
Observation	During the assessment it was observed that the application is using vulnerable NuGet.CommandLine version.
Severity Rating	Medium
Impact	Affected versions of this package are vulnerable to Resource Injection in the NuGetGallery backend job's handling of .nuspec files within NuGet packages. An attacker can bypass intended validation by supplying specially crafted package metadata (IDs or versions).
Recommendation	It is recommended to upgrade the NuGet.CommandLine to version 4.9.7, 5.11.7, 6.8.2, 6.11.2, 6.12.5, 6.14.3, 7.0.3, 7.3.1 or higher.
References	https://github.com/NuGet/NuGet.Client/security/advisories/GHSA-g4vj-cjjj-v7hg

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="EPPlus" version="8.4.2" targetFramework="net481" />
  <package id="EPPlus.Interfaces" version="8.4.0" targetFramework="net481" />
  <package id="ExcelDataReader" version="3.8.0" targetFramework="net481" />
  <package id="Microsoft.IO.RecyclableMemoryStream" version="3.0.1" targetFramework="net481" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="NuGet.Build.Tasks.Pack" version="6.14.0" targetFramework="net481" developmentDependency="true" />
  <package id="NuGet.CommandLine" version="7.3.0" targetFramework="net481" developmentDependency="true" />
  <package id="System.Buffers" version="4.5.1" targetFramework="net48" />
  <package id="System.Collections.Immutable" version="9.0.1" targetFramework="net48" />
  <package id="System.ComponentModel.Annotations" version="5.0.0" targetFramework="net481" />
  <package id="System.Memory" version="4.5.5" targetFramework="net48" />
  <package id="System.Numerics.Vectors" version="4.5.0" targetFramework="net48" />
  <package id="System.Runtime.CompilerServices.Unsafe" version="6.0.0" targetFramework="net48" />
  <package id="System.Security.Cryptography.Xml" version="8.0.2" targetFramework="net481" />
  <package id="System.ValueTuple" version="4.6.1" targetFramework="net481" />
</packages>
```

FIGURE 76: NUGET.COMMANDLINE 7.3.0

26. INSERTION OF SENSITIVE INFORMATION INTO LOG FILE

Path	RobilityActivities\Robility.Interact/packages.config: Robility.Interact@0.0.0 and Microsoft.Rest.ClientRuntime@2.3.20
Observation	During the assessment it was observed that the application is using vulnerable Microsoft.Rest.ClientRuntime version.
Severity Rating	**Medium**
Impact	**CVE-2022-26907:** Affected versions of this package are vulnerable to Insertion of Sensitive Information into Log File due to a lack of sanitization of exception messages.
Recommendation	It is recommended to upgrade the Microsoft.Rest.ClientRuntime to the latest version 2.3.24.
References	https://www.cve.org/CVERecord?id=CVE-2022-26907

Proof of Concept:

packages.config

```
<?xml ver
<packages>
  <package id="Azure.Core" version="1.50.0" targetFramework="net481" />
  <package id="Azure.Storage.Blobs" version="12.23.0" targetFramework="net481" />
  <package id="Azure.Storage.Common" version="12.26.0" targetFramework="net481" />
  <package id="Microsoft.AspNet.WebApi.Client" version="6.0.0" targetFramework="net481" />
  <package id="Microsoft.Azure.KeyVault.Core" version="3.0.5" targetFramework="net472" />
  <package id="Microsoft.Bcl.AsyncInterfaces" version="10.0.2" targetFramework="net481" />
  <package id="Microsoft.Extensions.Configuration.Abstractions" version="10.0.2" targetFramework="net481" />
  <package id="Microsoft.Extensions.DependencyInjection.Abstractions" version="10.0.2" targetFramework="net481" />
  <package id="Microsoft.Extensions.Diagnostics.Abstractions" version="10.0.2" targetFramework="net481" />
  <package id="Microsoft.Extensions.FileProviders.Abstractions" version="10.0.2" targetFramework="net481" />
  <package id="Microsoft.Extensions.Hosting.Abstractions" version="10.0.2" targetFramework="net481" />
  <package id="Microsoft.Extensions.Logging.Abstractions" version="10.0.2" targetFramework="net481" />
  <package id="Microsoft.Extensions.Options" version="10.0.2" targetFramework="net481" />
  <package id="Microsoft.Extensions.Primitives" version="10.0.2" targetFramework="net481" />
  <package id="Microsoft.Rest.ClientRuntime" version="2.3.20" targetFramework="net472" />
  <package id="Microsoft.Rest.ClientRuntime.Azure" version="3.3.18" targetFramework="net472" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="Newtonsoft.Json.Bson" version="1.0.3" targetFramework="net481" />
```

FIGURE 77: MICROSOFT.REST.CLIENTRUNTIME 2.3.20

27. RELIANCE ON UNDEFINED, UNSPECIFIED, OR IMPLEMENTATION-DEFINED BEHAVIOR	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-x64@7.20.0.1, Magick.NET-Q16-AnyCPU@7.12.0
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-x64 & Magick.NET-Q16-AnyCPU@7.12.0 version.
Severity Rating	**Medium**
Impact	Affected versions of this package are vulnerable to Reliance on Undefined, Unspecified, or Implementation-Defined Behavior due to undefined behavior in the clone_image operations when handling image data. An attacker can cause unintended modifications to files or partial denial of service by providing specially crafted image files.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-x64 Magick.NET-Q16-AnyCPU to version 14.8.0 or higher.
References	https://github.com/ImageMagick/ImageMagick/commit/63d8769dd6a8f32f4096c71be9e08a2c081e47da

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 78: MAGICK.NET-Q16-ANYCPU 7.12.0

28. ARBITRARY CODE INJECTION	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	**CVE-2026-25797:** Affected versions of this package are vulnerable to Arbitrary Code Injection in PostScript header processing. An attacker can execute malicious code by submitting a file that is processed by a printer or viewer.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-25797

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 79: MAGICK.NET-Q16-ANYCPU 7.12.0

29. MISSING RELEASE OF RESOURCE AFTER EFFECTIVE LIFETIME	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	**CVE-2026-25969:** Affected versions of this package are vulnerable to Missing Release of Resource after Effective Lifetime in ashlar.c(). An attacker can cause increased memory consumption and potential service disruption.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-25969

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 80: MAGICK.NET-Q16-ANYCPU 7.12.0

30. INCOMPLETE LIST OF DISALLOWED INPUTS

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	**CVE-2026-25966:** Affected versions of this package are vulnerable to Incomplete List of Disallowed Inputs in the form of blocking stdin and stdout but not blocking fd:* pseudo-filenames. An attacker can bypass the security policy to gain unauthorized access to standard input and output streams by supplying malicious commands that exploit this bypass.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-25966

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 81: MAGICK.NET-Q16-ANYCPU 7.12.0

31. UNCHECKED INPUT FOR LOOP CONDITION	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	Medium
Impact	**CVE-2026-25971:** Affected versions of this package are vulnerable to Unchecked Input for Loop Condition when handling MSL files. An attacker can cause a stack overflow and disrupt service availability by submitting malicious MSL files.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-25971

Proof of Concept:

packages.config

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <packages>
3    <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
4    <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
5    <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
6    <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
7    <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
8    <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
9    <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
10   <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
11   <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
12   <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
13   <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
14   <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
15   <package id="NLog" version="6.0.7" targetFramework="net481" />
16   <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
17   <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
18 </packages>
```

FIGURE 82: MAGICK.NET-Q16-ANYCPU 7.12.0

32. MISSING RELEASE OF MEMORY AFTER EFFECTIVE LIFETIME	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	**CVE-2026-25971:** Affected versions of this package are vulnerable to Unchecked Input for Loop Condition when handling MSL files. An attacker can cause a stack overflow and disrupt service availability by submitting malicious MSL files.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-25796

Proof of Concept:

packages.config

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <packages>
3    <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
4    <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
5    <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
6    <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
7    <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
8    <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
9    <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
10   <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
11   <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
12   <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
13   <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
14   <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
15   <package id="NLog" version="6.0.7" targetFramework="net481" />
16   <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
17   <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
18 </packages>
```

FIGURE 83: MAGICK.NET-Q16-ANYCPU 7.12.0

33. EXPIRED POINTER DEREFERENCE

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	**CVE-2026-25971:** Affected versions of this package are vulnerable to Unchecked Input for Loop Condition when handling MSL files. An attacker can cause a stack overflow and disrupt service availability by submitting malicious MSL files.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-25983

Proof of Concept:

packages.config

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <packages>
3    <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
4    <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
5    <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
6    <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
7    <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
8    <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
9    <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
10   <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
11   <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
12   <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
13   <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
14   <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
15   <package id="NLog" version="6.0.7" targetFramework="net481" />
16   <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
17   <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
18 </packages>
```

FIGURE 84: MAGICK.NET-Q16-ANYCPU 7.12.0

34. INTEGER UNDERFLOW (WRAP OR WRAPAROUND)	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	Affected versions of this package are vulnerable to Integer Underflow (Wrap or Wraparound) in the IPTC encoder. An attacker can access sensitive information or cause a partial denial of service by providing a specially crafted input file that triggers an out-of-bounds read.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.13.1 or higher
References	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-7wff-wpr6-vmhm

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 85: MAGICK.NET-Q16-ANYCPU 7.12.0

35. IMPROPER VALIDATION OF ARRAY INDEX	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	Affected versions of this package are vulnerable to Improper Validation of Array Index in the distort operation. An attacker can access sensitive memory contents or cause a partial denial of service by providing specially crafted arguments to the polynomial distortion operation.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.13.1 or higher
References	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-pfvh-m9xv-8966

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 86: MAGICK.NET-Q16-ANYCPU 7.12.0

36. INSECURE RANDOMNESS

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	Affected versions of this package are vulnerable to Insecure Randomness via the PasskeyEncipherImage function. An attacker can access sensitive information by exploiting AES-CTR nonce reuse during encryption.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.13.1 or higher
References	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-qv2q-c278-pch5

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 87: MAGICK.NET-Q16-ANYCPU 7.12.0

37. UNSYNCHRONIZED ACCESS TO SHARED DATA IN A MULTITHREADED CONTEXT	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	Affected versions of this package are vulnerable to Unsynchronized Access to Shared Data in a Multithreaded Context via a race condition in the distribute-cache process. An attacker can gain unauthorized access to file descriptors by connecting to the affected service during the race window.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.13.1 or higher
References	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-4g75-9r48-jf92

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 88: MAGICK.NET-Q16-ANYCPU 7.12.0

38. IMPROPER AUTHENTICATION

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	Medium
Impact	Affected versions of this package are vulnerable to Improper Authentication via the distribute-cache process. An attacker can access sensitive information or cause a denial of service by sending specially crafted requests to the service.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.13.1 or higher
References	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-6gxq-f64p-5w6f

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 89: MAGICK.NET-Q16-ANYCPU 7.12.0

39. INCORRECT CALCULATION OF BUFFER SIZE	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	Medium
Impact	**CVE-2026-25971:** Affected versions of this package are vulnerable to Unchecked Input for Loop Condition when handling MSL files. An attacker can cause a stack overflow and disrupt service availability by submitting malicious MSL files.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-26284

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 90: MAGICK.NET-Q16-ANYCPU 7.12.0

40. BUFFER ACCESS WITH INCORRECT LENGTH VALUE

Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	Medium
Impact	**CVE-2026-25971:** Affected versions of this package are vulnerable to Unchecked Input for Loop Condition when handling MSL files. An attacker can cause a stack overflow and disrupt service availability by submitting malicious MSL files.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-25986

Proof of Concept:

packages.config

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <packages>
3    <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
4    <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
5    <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
6    <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
7    <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
8    <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
9    <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
10   <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
11   <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
12   <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
13   <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
14   <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
15   <package id="NLog" version="6.0.7" targetFramework="net481" />
16   <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
17   <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
18 </packages>
```

FIGURE 91: MAGICK.NET-Q16-ANYCPU 7.12.0

41. DIVISION BY ZERO	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	**CVE-2026-25971:** Affected versions of this package are vulnerable to Unchecked Input for Loop Condition when handling MSL files. An attacker can cause a stack overflow and disrupt service availability by submitting malicious MSL files.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-25799

Proof of Concept:

packages.config

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <packages>
3    <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
4    <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
5    <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
6    <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
7    <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
8    <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
9    <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
10   <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
11   <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
12   <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
13   <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
14   <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
15   <package id="NLog" version="6.0.7" targetFramework="net481" />
16   <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
17   <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
18 </packages>
```

FIGURE 92: MAGICK.NET-Q16-ANYCPU 7.12.0

42. BUFFER OVER-READ	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	Medium
Impact	**CVE-2026-25971:** Affected versions of this package are vulnerable to Unchecked Input for Loop Condition when handling MSL files. An attacker can cause a stack overflow and disrupt service availability by submitting malicious MSL files.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-27798

Proof of Concept:

packages.config

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <packages>
3    <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
4    <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
5    <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
6    <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
7    <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
8    <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
9    <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
10   <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
11   <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
12   <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
13   <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
14   <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
15   <package id="NLog" version="6.0.7" targetFramework="net481" />
16   <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
17   <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
18 </packages>
```

FIGURE 93: MAGICK.NET-Q16-ANYCPU 7.12.0

43. IMPROPER ENCODING OR ESCAPING OF OUTPUT	
Path	RobilityActivities\Robility.SmartRPACognitiveServices/packages.config: Robility.SmartRPACognitiveServices@0.0.0 and Magick.NET-Q16-AnyCPU@7.12.0, Magick.NET-Q16-x64@7.20.0.1
Observation	During the assessment it was observed that the application is using vulnerable Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 version.
Severity Rating	**Medium**
Impact	**CVE-2026-25971:** Affected versions of this package are vulnerable to Unchecked Input for Loop Condition when handling MSL files. An attacker can cause a stack overflow and disrupt service availability by submitting malicious MSL files.
Recommendation	It is recommended to upgrade the Magick.NET-Q16-AnyCPU & Magick.NET-Q16-x64 to version 14.10.3. or higher
References	https://www.cve.org/CVERecord?id=CVE-2026-25543

Proof of Concept:

packages.config

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Google.Api.Gax" version="2.5.0" targetFramework="net452" />
  <package id="Google.Api.Gax.Rest" version="2.5.0" targetFramework="net452" />
  <package id="Google.Apis" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Auth" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Core" version="1.38.0" targetFramework="net452" />
  <package id="Google.Apis.Translate.v2" version="1.34.0.875" targetFramework="net452" />
  <package id="Google.Cloud.Translation.V2" version="1.1.0" targetFramework="net452" />
  <package id="Ionic.Zip" version="1.9.1.8" targetFramework="net481" />
  <package id="Magick.NET.Core" version="3.0.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-AnyCPU" version="7.12.0" targetFramework="net452" />
  <package id="Magick.NET-Q16-x64" version="7.20.0.1" targetFramework="net452" />
  <package id="Newtonsoft.Json" version="13.0.4" targetFramework="net481" />
  <package id="NLog" version="6.0.7" targetFramework="net481" />
  <package id="System.Interactive.Async" version="3.1.1" targetFramework="net452" requireReinstallation="true" />
  <package id="System.Net.Http" version="4.1.1" targetFramework="net452" requireReinstallation="true" />
</packages>
```

FIGURE 94: MAGICK.NET-Q16-ANYCPU 7.12.0

Annexure A – Source Code Review Methodology & Standards

Code review is systematic examination of source code and reviews are done in various forms and can be accomplished in various stages of each organization SDLC. The objective of this security assessment was to identify vulnerabilities in the source code which may possess potential vulnerabilities. The outcome of the static code analysis will help the development team to develop an action plan to minimize the risk in the web application.

- **Information Gathering**

  The objective of this phase is to get better understanding of the applications which helps in identifying business risks and possible threats to the application. It is carried out through reviewing / walking through of the application to understand the application & its features and identify critical and sensitive information it is handling.

- **Risk, Purpose & Context**

  It is essential to prioritize what features and components must be securely reviewed with a risk-based approach. While this highlights some of the vital areas of design security peer programmers should review all code being submitted to a repository and prioritize attention and scrutiny of a secure code review.

  Applications built have different purposes and therefore the evaluation of security will vary depending on the functionality being implemented. In each scenario, a payment web application will have higher security standards than a promotional website. Here, the priority and focus should be given of what the business wants to protect. Summary of the same is that a payment application, data such as credit cards will have the highest priority however in the case of a promotional website, one of the most important things to protect would be the connection credentials to the web servers. This is another way to place context into a risk-based approach. Persons conducting the security review should be aware of these priorities.

- **Lines Of Code**

  This phase indicates the amount of work that is the number of lines of code that must be reviewed during the assessments. IDEs (Integrated Development Environments) such as Visual Studio or Eclipse contain features which allows the number of lines of code to be calculated. The lines of code may or may not include third party code.

- **False Positive Analysis**

  In this phase, all the code segments are identified, analysed, and goes through manual review process. Team verifies the findings reported by Fortify tool to confirm existence of the vulnerability in the source code, prioritized them based on their criticality and impact. There is curated list provided in Annexure C. This list is prepared based on OWASP, well-known security vulnerabilities. Note, this list can update as and when required.

- **Reporting**

  After the completion of false positive analysis. True positives are reported, and an analyst prepares the derailed report consisting of the root cause, description, impact, and its remediation. External reference is provided wherever applicable.

Annexure B – TOOLS USED

Fortify - SCA	Fortify Static Code Analyzer (SCA) uses multiple algorithms and an expansive knowledge base of secure coding rules to analyze an application's source code for exploitable vulnerabilities. This technique analyzes every feasible path that execution and data can follow to identify and remediate vulnerabilities.

Annexure C – OWASP – Source Code Review

Below are the curated categories picked up from OWASP Code Review Guide to perform source code review.

List of Vulnerabilities
General
Cryptography
User Management
Same Origin Policy
Error Handling
Reviewing Logging Code
Authentication
Authorization
Session Management
Indirect Object Reference
Weak Input Validation
SQL Injection
Improper Error Handling
Web services
Cross-Site Scripting
Cross-Site Request Forgery
Using Components with Known Vulnerabilities
Injection Attacks
Open Redirection
Security Misconfiguration
XML Injection Attacks
Outdated Components used
Hardcoded Secrets
Undocumented Public Interface

Static Code Analysis Report

A REPORT BY CYBERPWN
EMPOWERING CYBER RESILIENCE

