Thick Client Application Testing Report

Prepared for: Sutherland Global Services Pvt Ltd

v1.1

March | 11 | 2024

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.

CONTENTS

DOCUMENT DETAILS

DOCUMENT CONTROL	
Document Title	**Thick-Client Penetration Testing Report**
Document Classification	Final Report
Last Edit Date	11-Mar-2024

DOCUMENT HISTORY			
DATE	**VERSION**	**PREPARED BY**	**STATUS**
07-Feb-2024	1.0	Sravan K	Final Report
11-Mar-2024	1.1	Sravan K	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	Vasu Sambandam
Title	Senior Associate Manager
Telephone	+91 - 9840897766
Email	vasu.sambandan@sutherlandglobal.com

CONSULTANT INFORMATION		
Name	**Role**	**Responsibility**
Sravan K	Lead Consultant	Document Preparation
Shruti MG	Lead Consultant	Document Review
Priti Mankar	Technical Manager	Document Approval
Swayam Prakash	CTO	Document Final Approval
Vasu Sambandam	Senior Associate Manager	Document Acceptance

INTRODUCTION

CyberPWN Technologies conducted **Thick-Client Penetration testing** for Robility Application. Based upon the Authorization to Test the application provided by the Company, Cyberpwn followed a testing methodology that sought to identify vulnerabilities and, through manual pentesting determine the impact to the Company's asset. Cyberpwn assigned a risk level based on goals achieved during testing.

SCOPE & DURATION

The scope includes **Thick-Client Penetration testing** for below mentioned target.

Application Name	Version
Robility_Designer	23.12.0.3
Robility_Runner	23.12.0.0

The test was performed from 19-Jan-2024 to 07-Feb-2024 including reporting.

Application Name	Version
Robility_Designer	24.0.7

The Re-test was performed from 11-Mar-2024 to 11-Mar-2024 including reporting.

LIMITATIONS & CONSTRAINTS

Testing occurred under the following constraints:

- The assessment was performed with the knowledge shared by the Sutherland team about the Robility application.
- The assessments were conducted from CyberPWN and the result(s) / finding(s) made are highly subjective to target system(s) and service(s) visibility and availability at that given point of time.

EXECUTIVE SUMMARY

CyberPWN was engaged by Client to conduct Thick Client application penetration testing of client's external interface facing system. The security assessment covered **RobilityDesigner.exe & RobilityRunner.exe** that was conducted from the CyberPWN offshore promise at Bangalore, India.

However, the assessment identified 01 Medium and 02 Low risks finding as an outcome of Thick client application penetration testing was performed internet facing system which were selected based on the operational criticality and the type of active network service.

- The 01 Medium and 2 Low rated risk is pertaining to vulnerabilities are Weak Encryption, Missing Security Headers, Server Version Disclosure, Rate Limiting is Not Implemented.

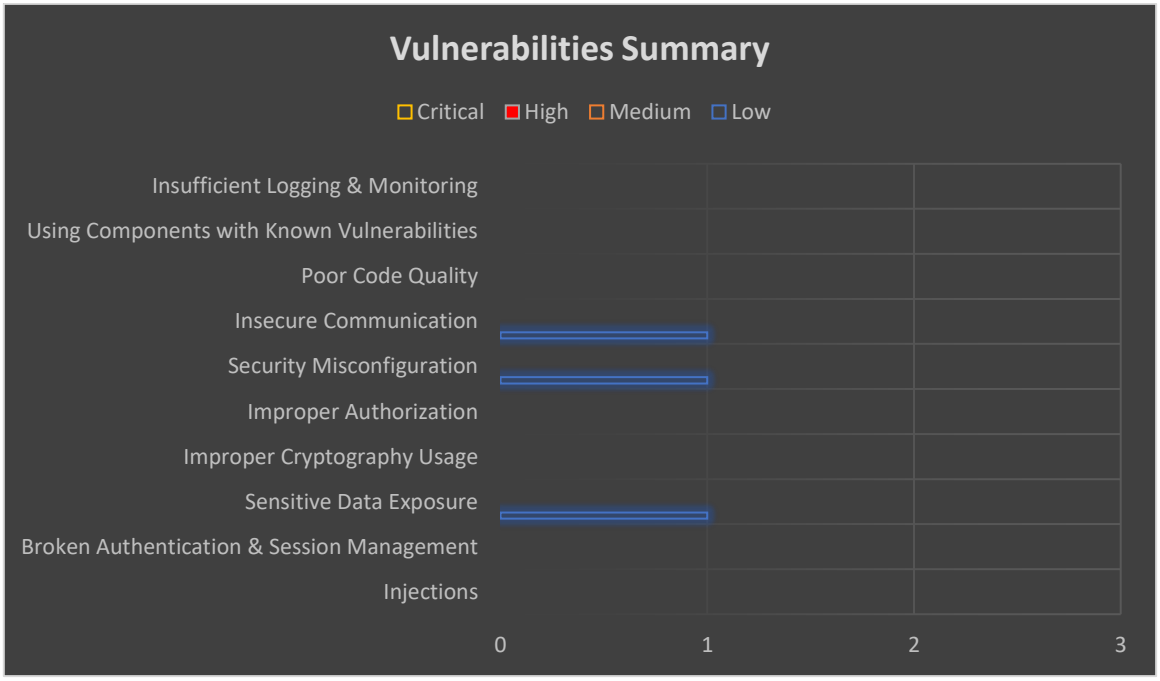
Summary of Finding

Total Vulnerabilities					
Critical	High	Medium	Low	Info	Total
0	0	01	02	0	03

Revalidation

Total Vulnerabilities					
Critical	High	Medium	Low	Info	Total
0	0	0	0	0	0

Finding Categorization



Introduction to Thick Client Penetration Testing:

Thick Client Penetration Testing focuses on evaluating the security of applications installed on end-user systems, encompassing desktop, mobile, or standalone software. This assessment aims to uncover vulnerabilities, weaknesses, and potential attack vectors in the application like memory corruption, race conditions, injection vulnerabilities, transport layer encryption weakness etc.

Vulnerability Scoring

A scoring system is used to grade all of the vulnerabilities listed in this report. CyberPWN employs the industry standard CVSSv3.1. It provides a system for determining the severity of vulnerabilities, regardless of the software/hardware platform or service function.

Every vulnerability is assigned a score between 0 and 10, giving each discovered vulnerability a score that aids in identifying the most vulnerable systems and prioritizing responses to each problem. The National Vulnerabilities Database (NVD) uses the CVSS system to calculate scores for almost all known vulnerabilities, and these are the scores referred to in this report.

Further information can be found at https://www.first.org/cvss/calculator/3.1

https://nvd.nist.gov/

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 Availability.
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

APPROACH AND METHODOLOGY

CyberPWN Technologies penetration testing methodology is based upon frameworks and standards mentioned below and it contains the following phases:

OWASP TOP 10
SANS TOP 25
The Penetration Testing Execution Standard (pentest-standard.org)
National Institute of Standards and Technology (NIST)
OSSTMM (Open Source Security Testing Methodology Manual)

PLANNING

- Cyberpwn Technologies prepares for initial planning sessions with the Company by reviewing the Company's business processes, key personnel, physical locations and Internet-accessible footprint.
- Cyberpwn Technologies and the Company collaborate to create the rules, attack scenarios, and goals for testing.
- The Company may provide additional documentation and access to applications, systems and networks to facilitate targeted testing.
- The Customer Company is responsible for ensuring that the scope contains all targets for testing and that the Company has the authority to permit Cyberpwn Technologies to perform penetration testing against the identified targets.

Thick client security assessment can be divided into below four major parts.

Static test

Source code decompilation

Based on the technology stack used to generate the binary file, one can attempt with a relevant decompiler to access the source code. For .Net, one can use ILSpy or dnSpy. Jd-gui or jadx for java based application. IDA Pro can be used for C/C++ with varied degree of success.

Code Injection

If an attacker is successful in decompiling the source code then attempt to introduce new or edit existing code to perform malicious actions such as a backdoor, etc. and recompile the application.

Configuration files in cleartext

If configuration and set-up files are in cleartext then they may contain information such as username, password, API key and other sensitive client server details. Report if such information found during inspection.

Test storage mechanism

Observe how the application is storing data at rest.

Dynamic test

Input validation

Test all input fields for issues such as SQL injection, command injection, buffer overflow, file system attack, etc.

Test File upload

If application provides file upload feature then test if an attacker can upload malicious custom file. Also, test how does application parses very big file size.

Broken authentication & session management

Test how application performs authentication and handles session management. Report the usage of weak password, possibility of user enumeration, improper session expiry, etc.

Log forging

If the application is maintaining logs then attempt to tamper log entries with malicious out-of-band payloads, spoof data, append large data to file, etc.

Weak GUI control

Inspect GUI controls of the application to learn if it is possible to enable additional/unintended features or options to current user. Tools that can aid in testing this are WinSpy++ and WinManipulate.

System test

Test for sensitive data in memory

Check RAM memory for how data is present when application is running. One can potentially find credential in cleartext and other important information. Winhex or ProcDump along with Volatility can extract and analyze memory.

Dependency mapping

An Attacker can use Process Explorer and ProcMon from SysInternals Suite to observe what dependency the application has.

Privilege level

Using icacls, one should check for privilege/permissions on the files and directories the thick client uses. If any excessive permission is provided , a missing .dll, DLL hijacking should be checked.

Network test

Testing transmission of sensitive data

Observe how data is passed over the wire. Report usage of sensitive data such as user credentials, personally identifiable information (PII), etc. transmitted in cleartext.

Testing weak encryption

Usage of weak encryption such as MD5, RC4, etc. may result in broken authentication, spoofing attack, key leakage and poor integrity of data in transit and must be reported.

Testing SSL/TLS usage

Check for presence of usage of weak cipher suites, security policies, deprecated protocols and misconfigurations.

REPORTING

Cyberpwn Technologies regularly communicates on the progress and results of testing during the engagement. Cyberpwn Technologies immediately notifies the Company if a critical-risk finding is discovered so that the Company can quickly remediate the issue.

Cyberpwn Technologies creates a report that contains, at minimum, the following items:

- **Executive Summary** - provides a high-level overview of the testing results and is intended to be read by executives, customers, and business partners.
- **Findings** - describes each exploitable vulnerability. The findings results are intended to be distributed
- to technical teams
- **Recommendations** - recommendations on how to resolve each identified issue
- **Risk Ranking** - each issue identified is assigned a risk ranking that is derived from the Common Vulnerability Scoring System (CVSS). The rating is based on the specific instances identified in the company environment.

- **Steps to Reproduce** - additional details that provide enough information such that the issue can be replicated by technical teams
- **Rescan** - updates about the finding, such as retesting status or management responses and revalidation report.

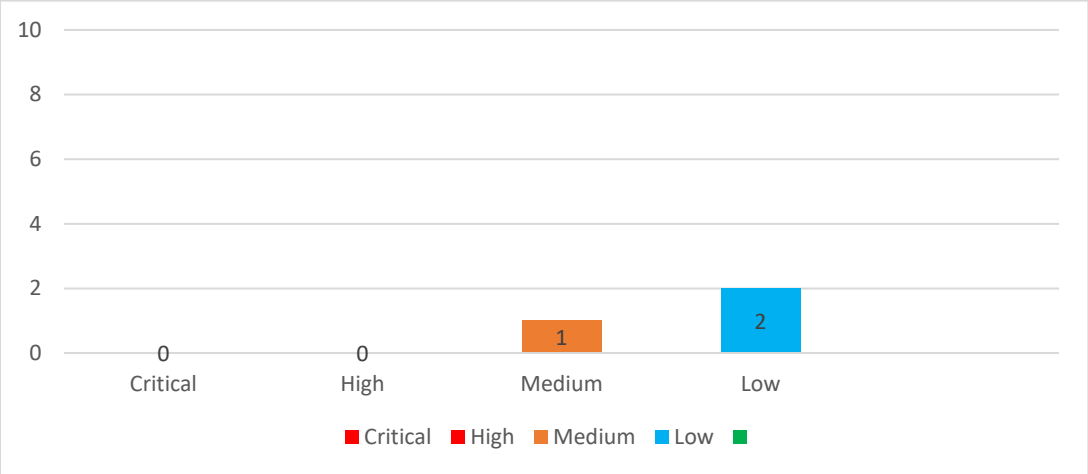
RESULT OVERVIEW

CyberPWN Technologies Security team discovered 03 risks and potential vulnerabilities in Robility Application.

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

SL. No.	Vulnerability Name	Severity Rating	Status
1.	INSECURE DATA STORAGE	MEDIUM	Exception [Closed]
2.	DEPRECATED TLS VERSIONS IN USE	Low	Remediated
3.	HARDCODED SECRETES	Low	Remediated

GRAPHICAL PRESENTATION



HIGH LEVEL RECOMMENDATIONS

The following recommendations offer guidance on enhancing the security posture of Robility Application:

1. Encrypt data at rest and in transit & Implement access controls
2. Disable the deprecated TLS versions: TLS 1.0 & 1.1.
3. Identify all hardcoded secrets & Store secrets securely.

After Revalidation all the vulnerabilities are closed

VULNERABILITIES DETAILS:

1. INSECURE DATA STORAGE	
Description	During the assessment it was observed that application is Storing the data in plain text format. We have designed Amazon s3 workflow to upload files to s3 bucket, The Accesskey and Secretkey stored in plain text format in the xaml file. Without proper encryption or protection mechanisms, sensitive data stored locally on the device can be easily accessed by unauthorized parties, leading to data breaches and privacy violations.
Revalidation Status	Exception [Closed] Note: Credential Vault has been used to store the secrets
Severity	Medium
CVSS Score	5.0
Application	RobilityDesigner.exe
Impact	Insecure data storage vulnerabilities in application pose a significant risk, potentially leading to severe consequences. Without adequate protection mechanisms, sensitive information stored locally on the device, such as login credentials, personal data, or financial details, becomes vulnerable to unauthorized access.
Remediation	• Do not hardcode credentials or keys. • The main approach in defending sensitive data is to use safe mechanisms to store and access information. • If at all it is necessary, then encrypt it with strong encryption mechanisms.
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N
Reference	https://www.owasp.org/index.php/Insecure_Storage

Proof of Concept:

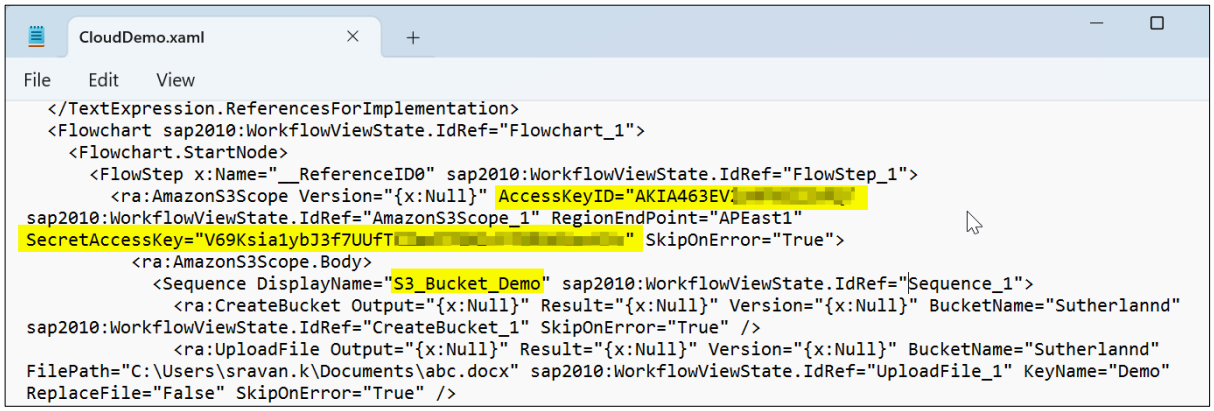
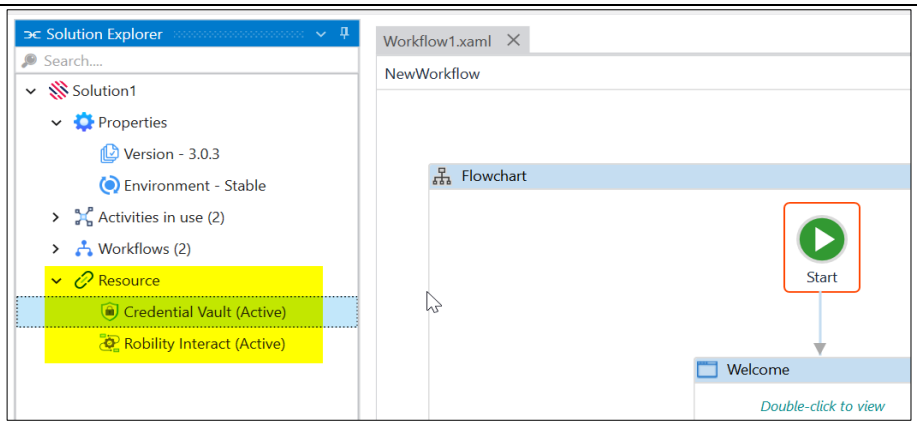


FIGURE 1: PLAIN TEXT DATA FROM XAML FILE.



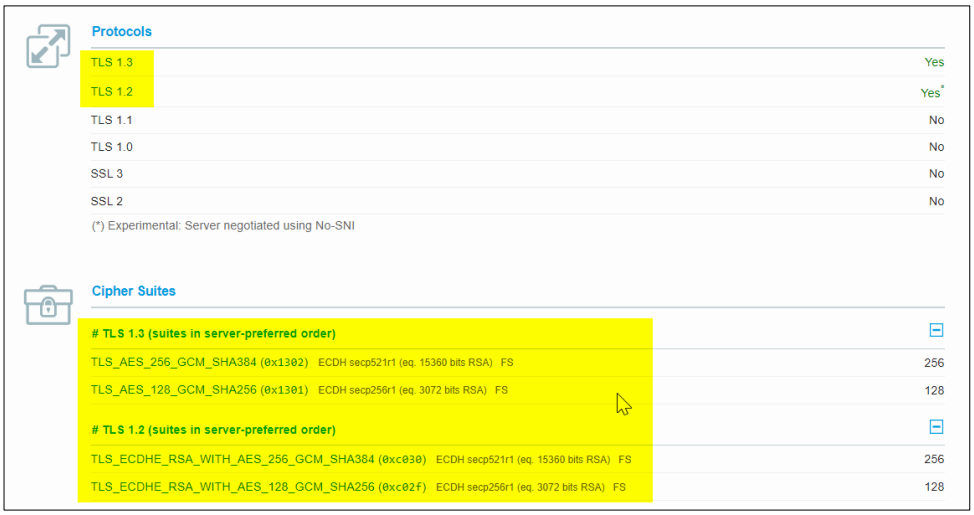
CREDENTIAL VAULT IS IN PLACE

2. DEPRECATED TLS VERSIONS IN USE	
Description	It was observed the web server allows for clients to use TLSv1.0 and TLSv1.1 protocol. These protocols are deprecated which are vulnerable to different attacks like LUCKY13 and BEAST. Insufficient Transport Layer Protection is a security weakness caused by applications not taking any measures to protect network traffic. During authentication applications may use SSL/TLS, but they often fail to make use of it elsewhere in the application, thereby leaving data and session IDs exposed. Exposed data and session ID's can be intercepted which means the application is vulnerable to exploit. Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.
Revalidation Status	Remediated
Severity	Low
CVSS Score	2.9
Application	RobilityDesigner.exe
Impact	Using deprecated TLSv1.0 and TLSv1.1 protocols poses severe security risks, including weak encryption, known vulnerabilities like BEAST and POODLE, absence of modern security features, compliance challenges, compatibility issues with modern software, susceptibility to man-in-the-middle attacks, increased likelihood of data breaches, and limited defense against evolving cyber threats. Upgrading to more secure protocols is crucial to mitigate these risks and ensure data confidentiality and integrity.
Remediation	It is recommended to: • Disable support for TLSV 1.0 & TLS 1.1 on the server. • should use the latest stable version of TLS v1.2 and TLSV 1.3.
CVSS String	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
Reference	https://datatracker.ietf.org/doc/html/rfc8996
Proof of Concept:	

```
Testing SSL server 40.112.243.101 on port 443 using SNI name 40.112.243.101

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-521 DHE 521
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-521 DHE 521
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-521 DHE 521
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-521 DHE 521
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  128 bits  AES128-SHA
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-521 DHE 521
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA
```

FIGURE 2: DEPRECATED TLS 1.0 & 1.1 IN USE



REVALIDATION POC – TLS V1.2 AND V1.3 ARE USED WITH STRONG CIPHERS.

3. Hardcoded Credentials in use	
Description	It was observed during the assessment that application has Hard-Coded Credentials. The credentials contain Username, Password, Key and DB Name.
Revalidation Status	Remediated
Severity	Medium
CVSS Score	2.0
Application	RobilityDesigner.exe
Impact	The use of hard-coded credentials is considered to be a security risk because it makes it easy for an attacker to access sensitive information if they are able to obtain access to the source code. If the source code is made public, for example through a software repository like GitHub, the hard-coded credentials can be easily found and used by unauthorized parties.
Remediation	It is Recommended to • Use encryption: Encrypting sensitive information and systems can help prevent attackers from accessing this information if hard-coded credentials are exploited. • Limit access to sensitive information: Limiting access to sensitive information to only those who need it can reduce the risk of this information being accessed or misused in the event of a breach.
CVSS String	CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N
Reference	https://cwe.mitre.org/data/definitions/798.html

Proof of Concept:

```
  <Marketplace>
    <M_Address Value ="https://robility.sutherlandglobal.com/HubAPI/"/>
    <M_Username Value="vas"/>
    <M_Password  Value="Smart[redacted]123"/>
    <M_key  Value="EE1FD335[redacted]"/>
    <M_DBName  Value="Robility"/>
  </Marketplace>
</Designer>
```

FIGURE 3: DETAILS FROM VAULT.XML FILE

```
<?xml version="1.0" encoding="utf-8"?>
<Designer>
  <ManagerURL>
    <RobilityManagerSignIn Value=
    "nYcXGpGZA7cUGqyMBRb1cjxbuhha7ti6cK7SAO160vwY57dDO0ao4QtPQezjsyRIgMc+k6pZFEiDk
    dLB+RYL1Z0FvLRYCpXzXoqVr3g0/SFDO8I7VpVY71vUy1mZDqrKWRsVhAHxMgbcdVVVABxA==" />
    <DesignerService Value=
    "vGkC4zEf+o1XN0wQW+3PGZnF/zlAk+AVUHnuNtP419ICGzzj1spVWyB8X7MI7E4QzP702wQ/UZdaW
    uui40zZyQAYZowsuc5rAGnGez3imijW9qaiQySa+mtbJGVPRDx+a05gEieqnEwcDj/z7flA==" />
    <FeatureService Value=
    "JurAerDp2xl7HX42p4yO8KA0ZuRWddtZgtHr5OsK3IP2MrJdiVwCeR9qcEDrm40RiOzUQk9eHcrY9
    mT1j4YO9yJbqoQo3CxcCSbduvEGylLLihtrJjXJQ0Xb3Uo81N3DAahjInj/PRnDb3UvIkPg==" />
    <RunnerService Value=
    "Qp9mD7UUfNLLZVl3brMQkkwnumukncmUFKQ0gk7z7ndTjS4VbMAjgoIGBJqpi9XkUX/gLCZGqUJCq
    A/4y4NKUQ3BooQYUcSmj4kMpNsrY=" />
```

REVALIDATION POC: DETAILS ARE ENCODED

CONCLUSION

Our security assessment revealed 03 vulnerabilities in the **Robility** Application, issues are related to Insecure Data Storage, Deprecated TLS Versions In Use and Hardcoded Secretes.

After Revalidation all the vulnerabilities are closed

Annexure A – CHANGES TO ENVIRONMENT

No changes were made to the environment in scope, such as creating new user accounts or uploading files to the target system.

Annexure B – TOOLS USED

Microsoft Sys-internal tools	Suite of powerful utilities for system management, troubleshooting, and analysis in Windows environments https://docs.microsoft.com/en-us/sysinternals/
EchoMirage	A Network proxy tool, used for DLL injection and function hooking techniques to redirect network related function calls so that data transmitted and received by local applications.
BurpSuite	Burp Suite is a Java based Web Penetration Testing framework. It has become an industry standard suite of tools used by information security professionals. Burp Suite helps you identify vulnerabilities and verify attack vectors that are affecting web applications
SSLSCAN	The SSL Scanner uses a scanning engine based on the *testssl.sh* tool, together with multiple tweaks, adjustments, and improvements. The scanner works by connecting to the target SSL server and trying various ciphers and SSL/TLS protocol versions to determine existing vulnerabilities.
Metasploit	Metasploit is an open-source tool is used to probe systematic vulnerabilities on networks and servers.
WireShark	Wireshark is a network traffic analyzer, or "sniffer", for Unix and Unix-like operating systems.
Netspy	A tool to quickly detect the reachable network segments of the intranet
Kali Linux	Used to initiate advanced-level Security Auditing and Penetration Testing.
Customer Exploit Scripts	

Annexure C - LIST OF VAPT TESTS PERFORMED

Test Cases
Recon
Fingerprinting
Authentication and Authorization
Input Validation and Manipulation
Insecure Data Storage
Network Communication
Memory Corruption and Buffer Overflows
Code Execution and Arbitrary File Upload
Session Management
Cryptography
Client-Side Security
Unvalidated Redirects and Forwards
Error Handling and Information Disclosure
Application Logic
Third-Party Integration