**Vulnerability Assessment Report**

**29th of September, 2023**

# System Description

On September 28, 2023, we conducted Nessus scans using a Kali Linux machine on premises. Nessus permits scanning up to 16 IP addresses simultaneously, and for this assessment, we utilized IP addresses in the range of X.X.X.X. The results of the scan revealed the following counts of alerts:

* - 7 critical alerts
* - 12 high alerts
* - 73 medium alerts
* - 16 low alerts
* - 449 alerts categorized as none

# Scope

The assessment aims to identify and evaluate potential security vulnerabilities within the target environment. This document serves as a guide for the assessment process, ensuring a comprehensive and effective evaluation of the systems and network. Nessus will be used to conduct the vulnerability assessment. The assessment will include:

**Network Scanning:** Identify open ports, services, and vulnerabilities on networked devices.

**Credential-based Scanning:** Authenticate scans for a more comprehensive assessment of hosts and systems.

**Web Application Scanning:** Perform in-depth scanning of web applications to identify vulnerabilities like SQL injection, Cross-Site Scripting (XSS), and more.

**Compliance Checks:** Evaluate the target environment's compliance with industry-specific security standards (if applicable).

# Purpose

The vulnerability assessment will focus on the following aspects of the target environment:

**Network Infrastructure:** Evaluate the security of network devices, routers, switches, firewalls, and related infrastructure components.

**Servers and Endpoints:** Scan servers (both physical and virtual) and endpoints (workstations, laptops) for vulnerabilities in the operating system and installed software.

**Web Applications:** Assess the security of web applications, including web servers, web application frameworks, and associated databases.

**Third-party Software:** Identify vulnerabilities in third-party applications and services utilized within the target environment.

**Configuration Weaknesses:** Evaluate the security configuration of systems and devices, including password policies, access controls, and encryption settings.

# Risk Assessment

Here is a prioritized list of Critical and High-priority items that should be addressed first.

|  |  |  |  |
| --- | --- | --- | --- |
| **Host source** | **Threat event** | **Protocols** | **Solutions** |
| *Host: X.X.X.X*  *Port: 1433, 3389, 1801* | * *SSL Version 2 and 3 Protocol Detection* * *SSL Certificate Signed Using Weak Hashing Algorithm* * *SSL Medium Strength Cipher Suites Supported (SWEET32)* * *Microsoft SQL Server Unsupported Version Detection (remote check)* * *Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper)* | *TCP* | * *Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.* * *Contact the Certificate Authority to have the SSL certificate reissued.* * *Reconfigure the affected application if possible to avoid use of medium strength ciphers.* * *Upgrade to a version of Microsoft SQL Server that is currently supported.* * *Apply updates in accordance with the vendor advisory.* |
| *Host: X.X.X.X*  *Port: 4343, 54051, 3389* | * *SSL Version 2 and 3 Protocol Detection* * *SSL Certificate Signed Using Weak Hashing Algorithm* * *SSL Medium Strength Cipher Suites Supported (SWEET32)* * *Microsoft SQL Server Unsupported Version Detection (remote check)* | *TCP* | * *Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.* * *Contact the Certificate Authority to have the SSL certificate reissued.* * *Reconfigure the affected application if possible to avoid use of medium strength ciphers.* * *Upgrade to a version of Microsoft SQL Server that is currently supported.* |
| *Host: X.X.X.X*  *Port: 3389* | * *SSL Certificate Signed Using Weak Hashing Algorithm* * *SSL Medium Strength Cipher Suites Supported (SWEET32)* | *TCP* | * *Contact the Certificate Authority to have the SSL certificate reissued.* * *Reconfigure the affected application if possible to avoid use of medium strength ciphers.* |
| *Host: X.X.X.X*  *Port: 3389* | * *SSL Medium Strength Cipher Suites Supported (SWEET32)* | *TCP* | * *Reconfigure the affected application if possible to avoid use of* |

# Approach

# Following the resolution of High and Critical alerts, we advise reviewing the Medium and Low alerts to assess their potential impact on Pueblo Library's systems. It's possible that some alerts may not necessitate additional action or may be addressed while addressing the critical and high-priority alerts. After resolving the critical and high alerts, we will conduct another Nessus scan to determine if these issues still persist.

# Remediation Strategy

The following actions are recommended for immediate attention:

1. Implementing application updates and server updates.

2. Disabling unnecessary services to restrict server access to authorized users only.

3. Enhancing data security by transitioning from SSL to TLS encryption for data in motion.

4. Reconfiguring affected server accounts and disabling unnecessary services to mitigate critical and high-priority alerts.

5. Once the issues have been addressed, conduct another Nessus scan to reassess the situation.