Cyber Risk Assessment

The City of Suffolk, Virginia
Information Technology Department

November 19th, 2024

Old Dominion University

Commonwealth Cyber Initiative Coastal Virginia

Team A

A graduating senior from the Old Dominion University School of Cyber Security. He is currently interning with COVA CCI in partnership with Valor Cybersecurity providing services for The City of Suffolk. His role coordinated team members, dates, communication, and led project development.

A sophomore from the Old Dominion University School of Cyber Security. He is currently interning with COVA CCI in partnership with Valor Cybersecurity providing services for The City of Suffolk. His role provided support as needed and performed analysis and assessment of compliance settings.

A junior from the Old Dominion University School of Cyber Security. He is currently interning with COVA CCI in partnership with Valor Cybersecurity providing services for The City of Suffolk. His role provided analysis and assessment of identified risks.

Team B

A graduating senior majoring in Cybercrime at Old Dominion University, is currently interning with COVA CCI in partnership with Valor Cybersecurity. In her role, she provided key support in communicating with the City of Suffolk, where she conducted a risk assessment of their SQL database, classifying and analyzing potential risks.

A senior majoring in Cybersecurity at Old Dominion university, is currently interning with COVA CCI in partnership with Valor Cybersecurity. In his role, he provided secondary communications with the City of Suffolk, where he analyzed identified risks of their SQL database and provided recommendations for remediation.

A graduating senior majoring in Cybersecurity at Old Dominion University, is currently interning with COVA CCI in partnership with Valor Cybersecurity. In his role, he contributed to compliance in a risk assessment conducted on the City of Suffolk's SQL database where he documented gaps offering recommendations for remediations to meet industry standards.

Overview of IT Department of The City of Suffolk, VA

The Information Technology (IT) Department of Suffolk, VA is responsible for supporting the city's technological infrastructure, ensuring secure and reliable networks, managing communications, providing technical support to city departments, and ensuring the efficiency of municipal operations. It focuses on cybersecurity, data management, and maintaining up-to-date technology for the city’s services.

Project objective:

To conduct a comprehensive risk assessment of the City of Suffolk’s SQL database and Public Windows Server using Tenable.io, identifying vulnerabilities, evaluating potential impacts, and providing actionable recommendations to enhance the security posture of the databases.

This assessment aims to support the city in maintaining the confidentiality, integrity, and availability of critical data, ensuring compliance with relevant security standards and improving overall cybersecurity resilience.

Tenable.io overview

Tenable.io is a cloud-based vulnerability management platform that enables organizations to continuously identify, assess, and manage cybersecurity risks across their network. It provides real-time visibility into vulnerabilities, configuration issues, and compliance risks for assets such as servers, applications, and databases.

By prioritizing vulnerabilities based on risk, Tenable.io helps organizations address security gaps, improve their overall security posture, and maintain compliance.

Assessment Scope

System analyzed

System overview: The assessments focused on a SQL database hosted on a Windows Server environment and a Windows Server 2012 R2 (public web server), which are integral to the City's data management and operations.

Database Type: Microsoft SQL Server 2012 & Windows Server 2012 R2.

Assessment Methodology

Scanning and Analysis: Initial vulnerability scan conducted through Tenable.io to identify vulnerabilities within the Windows 2012 R2 & SQL database environment.

Risk Prioritization: Analysis of identified vulnerabilities based on severity and impact, with a focus on addressing the critical vulnerabilities first.

Remediation: Developed remediation steps so that security improvements were effectively implemented.

Scope of the risk assessment

The scope of both servers conducted in Tenable.io focused on identifying vulnerabilities, misconfigurations, and security gaps within the database environment. This approach provided a clear path for remediation and prioritized protection for the servers.

Cyber Risk Assessment
The City of Suffolk, Virginia
Windows Server

Edwin Wells, Brayden Greenfield, Niko Florido

November 19, 2024

Findings in Tenable.io: Cyber Exposure Score

Score of 645

17 solutions will reduce score to 0 and eliminate 18 CVE instances across 87 CVE's.

Findings in Tenable.io: Vulnerabilities Identified

Critical Vulnerabilities - 4 total

Average Age 250 Days

Ranges from 28 - 547 days

Does not meet self set standards

High Vulnerabilities - 8 total

Average Age 224 Days

Ranges from 9 - 547 days

Does not meet self set standards

Findings in Tenable.io: Critical Vulnerabilities

KB5044343: Windows Server 2012 R2 Security Update (October 2024)

- The remote Windows host is affected by multiple vulnerabilities.
    - 50 CVE’s were found

Progress OpenEdge 11.7.x < 11.7.19 / 12.2.x < 12.2.13 / 12.8.x < 12.8.1 (000253075)

- The remote host is missing a security update.

Oracle Java JRE Unsupported Version Detection

- The remote host contains one or more unsupported versions of the Oracle Java JRE.

Microsoft Windows Server 2012 SEoL

- An unsupported version of Microsoft Windows is installed on the remote host.

Recommended Mitigations: Critical Vulnerabilities

KB5044343: Windows Server 2012 R2 Security Update (October 2024)

- Apply Security Update 5044343.
- Eliminate 50 CVE Instances across the total of 87 CVEs.

Progress OpenEdge 11.7.x < 11.7.19 / 12.2.x < 12.2.13 / 12.8.x < 12.8.1 (000253075)

- Update to version 11.7.19 / 12.2.13 / 12.8.1 or later.

Oracle Java JRE Unsupported Version Detection

- Upgrade to a supported version.

Microsoft Windows Server 2012 SEoL

- Upgrade to a supported version.

Findings in Tenable.io: High Vulnerabilities

Top 3

Windows PrintNightmare Registry Exposure CVE-2021-34527 OOB Security Update RCE (July 2021)

- The remote Windows host is affected by a remote code execution vulnerability.

VMware Tools 10.3.x / 11.x / 12.x < 12.3.5 Token Bypass (VMSA-2023-0024)

- The virtualization tool suite is installed on the remote Windows host is affected by an authentication bypass vulnerability.

Azul Zulu Java Multiple Vulnerabilities (2024-11-12)

- Azul Zulu OpenJDK is affected by multiple vulnerabilities.
  - 6 CVE’s were found

Recommended Mitigations: High Vulnerabilities | Top 3

Windows PrintNightmare Registry Exposure CVE-2021-34527 OOB Security Update RCE (July 2021)

- Perform security updates and confirm that registry settings are set to zero or are not defined per CVE recommendations.

VMware Tools 10.3.x / 11.x / 12.x < 12.3.5 Token Bypass (VMSA-2023-0024)

- Upgrade to version 12.3.5 or later.

Azul Zulu Java Multiple Vulnerabilities (2024-11-12)

- Apply patch from the November 2024 Azul Zulu OpenJDK Patch Update advisory.

Findings in Tenable.io: High Vulnerabilities

Bottom 3

SSL Medium Strength Cipher Suites Supported (SWEET32)

- The remote service supports the use of medium strength SSL ciphers.

Security Updates for Microsoft .NET Framework (October 2024)

- The Microsoft .NET Framework installation on the remote host is missing a security update.

Apache Shiro before 1.11.0 Authentication Bypass

- A Java security framework is affected by an authentication bypass vulnerability.

Recommended Mitigations: High Vulnerabilities | Bottom 3

SSL Medium Strength Cipher Suites Supported (SWEET32)	● Reconfigure to use stronger ciphers.
Security Updates for Microsoft .NET Framework (October 2024)	● Install missing security update.
Apache Shiro before 1.11.0 Authentication Bypass	● Upgrade to 1.11.0 or later.

What is the CIS compliance standard?

“Center for Internet Security (CIS) are a set of globally recognized and consensus-driven best practices to help security practitioners implement and manage their cybersecurity defenses.”

Why is it Important to be Compliant

- Lowers exposure to cybersecurity risk
- Aids in preventing data breaches
- Meeting agreements

Windows Compliance and Security Standards

Compliance Type	Status	Count
CIS Windows	Failed	48
	Passed	3

Recommend Compliance Changes (Easy)

18.9.48.1 (L2) Ensure 'Turn off the advertising ID' is set to 'Enabled'

- This policy setting turns off the advertising ID, preventing apps from using the ID for experiences across apps.

18.9.20.1.12 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'

- This policy setting specifies whether the Windows Customer Experience Improvement Program can collect anonymous information about how Windows is used.

18.10.37.2 (L2) Ensure 'Turn off location' is set to 'Enabled'

- This policy setting turns off the location feature for the computer.

Recommend Compliance Changes (Hard)

18.8.37.2 Ensure 'Restrict Unauthenticated RPC clients'

- This policy setting controls how the RPC server runtime handles unauthenticated RPC clients connecting to RPC servers.
- Set to **Enabled: Authenticated.**

18.6.19.2.1 (L2) Disable IPv6

- If IPv6 is not required for this machine than it recommended that it is **disabled.**

18.10.89.2.2 (L2) Ensure 'Allow remote server management through WinRM'

- This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port.
- It is recommended to **disable** WinRM.

Up Next:

Team B

Cyber Risk Assessment

SQL Database

Cyber Risk Assessment

The City of Suffolk, Virginia

SQL database

Rebecca Hight, Micah Elmore, David Levy

November 19th, 2024

Findings in Tenable.io: Vulnerabilities Identified

- **Scans completed:** Advanced Network Scan, Malware Scan, and Policy Compliance Auditing Scan.

- Total of 208 findings

Critical: 10

High: 26

Medium: 29

Low: 9

Info: 134

Cyber Exposure Score: 816

15 solutions will reduce the cyber score to 0, eliminating 18 CVE instances across 80 CVE’s.

Risk Impact: Critical Vulnerabilities | Top 3

KB5044342, KB5041851, KB5040485, KB5043125, KB5032247, KB5039260: Windows Server 2012 Security Update

- The remote Windows host is missing security updates. It is, therefore, affected by multiple vulnerabilities.

SSL Version 2 and 3 Protocol Detection

- The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0.

Microsoft SQL Server Unsupported Version Detection

- The installation of Microsoft SQL Server on the remote host is no longer supported.

Recommended Mitigations: Critical Vulnerabilities | Top 3

KB5044342, KB5041851, KB5040485, KB5043125, KB5039260,KB5032247: Windows Server 2012 Security Update	● Apply security updates: KB5044342, KB5041851, KB5040485, KB5043125, KB5039260, KB5032247.
SSL Version 2 and 3 Protocol Detection	● Disable SSL2.0 & 3.0. Start using TLS 2.1 or higher.
Microsoft SQL Server Unsupported Version Detection	● Upgrade to a version of Microsoft SQL Server that is currently supported.

Risk Impact: High Vulnerabilities | Top 3

Windows PrintNightmare Registry Exposure (CVE-2021-34527)

- A remote command execution vulnerability exists in Windows Print Spooler service improperly performs privileged file operations.

Vim < 9.0.2010 Use-After-Free

- Memory is accessed after it has been freed, allowing attackers to execute code or cause a program crash.

VMware Tools 10.3.x / 11.x / 12.x < 12.3.5 Token Bypass (VMSA-2023-0024)

- The current version of VMware tools is out of date. It is, therefore, affected by a SAML token signature bypass vulnerability.

Recommended Mitigations: High Vulnerabilities | Top 3

Windows PrintNightmare Registry Exposure CVE-2021-34527 OOB Security Update RCE (July 2021)	● Ensure that the latest out-of-band security updates from Microsoft are applied to your Windows systems. Microsoft released patches to address this vulnerability.
Vim < 9.0.2010 Use-After-Free	● Contact the Certificate Authority to have the SSL certificate reissued.
VMware Tools 10.3.x / 11.x / 12.x < 12.3.5 Token Bypass (VMSA-2023-0024)	● Upgrade to VMware Tools version 12.3.5 or later.

Risk Impact: High Vulnerabilities | Bottom 3

SSL Medium Strength Cipher Suites Supported (SWEET32) (Port # 3389 and Port # 1433)

- The remote host supports the use of SSL ciphers that offer medium strength encryption. It is easier to circumvent medium strength encryption if the attacker is on the same physical network.

Security Updates for Internet Explorer

- The Internet Explorer installation on the remote host is missing security updates. It is, therefore, affected by multiple vulnerabilities.

VMWare Tools < 12.1.0 Privilege Escalation

- A malicious actor with local non-administrative access to the Guest OS can escalate privileges as a root user in the virtual machine.

Recommended Mitigations: High Vulnerabilities | Bottom 3

Internet Explorer Updates	● Microsoft has released security updates for the affected versions of Internet Explorer.
VMware Tools 11.x / 12x < 12.1.0 Privilege Escalation (VMSA-2022–0024)	● Upgrade to VMware Tools version 12.1.0 or later.
SSL Medium Strength Cipher Suites Supported (SWEET32) Port # 3389 and Port # 1433	● Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Compliance and Security Standards

- **Objective:** Evaluate adherence to CIS compliance standards for Windows SQL
- **Standards Assessed:** CIS Windows Server 2012 MS L2 v3.0.0
- **Scan Results:**

Compliance Type	Status	Count
CIS Windows	Failed	48
	Passed	1

- **Remediation:** Group Policy (GP) configurations need adjustments. Each failed check's recommended configuration states a specific "UI path" within the Group Policy editor that needs to be set to either "Enabled” or “Disabled.”

Combined Conclusion

Key Strategies:

- Upgrade, patch, and maintain software and applications
- Transition to supported hardware
- Address failed CIS benchmarks

THANK YOU FOR HOSTING US AT SUFFOLK CITY HALL