Mitigating Known Vulnerabilities within SLTT Government Networks

Publication: November 2022

Cybersecurity and Infrastructure Security Agency

Table of Contents

Tables

Introduction

This document serves as a supplement to CISA's Cyber Risk Summary (CRS) on the SLTT Government Facilities Sector[1] and provides an in-depth analysis of known vulnerabilities and defensive mitigation strategy recommendations to aid in minimizing risks associated with SLTT cyber assets.

Published in April 2022, the SLTT Government Facilities Sector CRS provides an analysis of findings for SLTT government facilities[2] subscribed to CISA services based on 2021 data. The CRS recommends supporting mitigations for SLTT governments to consider when evaluating cybersecurity posture and capabilities.

CISA created this supplement to the CRS to provide SLTT government facility personnel—including information technology (IT)/operational technology (OT) security teams and executive decision makers—assistance in evaluating existing cyber hygiene practices. Additionally, this supplement aims to aid SLTT government in applying appropriate security measures to preserve their most valuable assets.

The following section describes known vulnerabilities CISA found on internet-accessible hosts and systems across SLTT government networks.

SLTT Known Vulnerability Analysis

This supplement further analyzes the vulnerability findings identified within the CRS and provides (1) descriptive scenarios that detail how a threat actor may exploit a weakness, and (2) mitigation strategies that SLTT governments should apply to secure and reduce known risks for SLTT government facility networks.

Each scenario contains the following contextual information:

- **Vulnerability name** – name of the weakness identified
- **Vulnerability description** – explanation of how the weakness could be exploited or triggered by a threat source
- **Intended target** – vulnerable IT/OT assets, endpoints, and/or users on the network that are susceptible to compromise
- **Complexity to exploit** – level of difficulty to exploit the weakness/vulnerability
- **Method of attack** – path or method the threat actor uses to gain unauthorized access to a system or network by exploiting vulnerabilities

[1] The Cyber Risk Summary: SLTT Government Facilities Sector is a TLP:AMBER product, and authorized recipients can reach out to your regional cybersecurity advisor and/or MS-ISAC correspondent for access.
[2] This summary uses data collected from SLTT Governments Facilities as defined in the Government Facilities Sector Specific Plan. SLTT Government Facilities will be referred to as SLTT governments throughout the rest of this report and do not include Education, Election, or Emergency Services Sector entities.

- **Threat actor gain** – value the threat actor can potentially gain (e.g., access, information, the ability to affect/deny access to the system, etc.) from the weakness/vulnerability
- **Mitigation recommendations** – technical recommendations and solutions suggested to secure endpoints on an entity's network
- **CISA resources and services** – CISA services and offerings available to SLTT Government Facilities Sector organizations

Potential Effects of Bad Practices on Networks

Tables 1 through 5 provide several scenarios outlining the potential effects of bad IT practices on SLTT government networks and their associated IT/OT assets.

Table 1: Phishing Susceptibility Scenario

Phishing is a technique used by threat actors to gain network access by exploiting users who are susceptible to responding to a phishing email or clicking a phishing link. Phishing depends on tricking the user into providing sensitive information or accessing a malicious file or link to deliver and execute malware. Successful phishing attempts depend on email servers that fail to block delivery, users that are susceptible to interacting with malicious files or links, applications or browsers that are susceptible to malicious code, and endpoint security software that fails to detect and block malware.	
Intended Target	End users
Complexity to exploit	Exploitation complexity varies; social engineering attacks like phishing were the most prevalent type of attack vector that led to compromise in 2021.[3] Additionally, phishing as a service (PhaaS) may affect the complexity to exploit, as it lowers the barriers to carrying out a phishing attack.
Method of attack	• Delivery of socially engineered emails containing malicious links and/or files • Delivery of socially engineered emails soliciting various pieces of sensitive information (e.g., financial information, personal profiling data [passwords], etc.)
Threat actor gain	• Access to device and organizational data • Enables successful distribution of malicious files
Mitigation recommendations	To prevent a successful phishing attack: • Implement Multifactor Authentication (MFA) for all authentication requests to prevent unauthorized access resulting from compromised credentials

[3] https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-ransomware-survey.pdf

	○ While any MFA is better than no MFA, research phishing resistant FIDO authentication (also called WebAuthn) ○ See CISA.gov/MFA for additional resources and MFA options. • Be sure to update end user operating systems, browsers, and applications • Deploy antivirus (AV) with automated AV updates • Implement EDR solutions to block potentially malicious activity, or application allowlisting • Implement edge firewalls and configure to alert on potentially malicious web interactions • Provide extensive security awareness training, to ensure end users are aware of and can identify phishing scams • Develop and implement a process to enable end user reporting of suspected phishing attempts for further review by security operations ○ Ensure security operations analysts extract information from verified phishing attempts for incorporation in detections and defenses To limit the impact of a successful phishing attempt: • Monitor and log network and mail server activity and endpoint processes for abnormal and potentially malicious activities • Implement zero trust and remove administrator rights from user devices to limit a threat actor's ability to move laterally throughout a compromised network • Maintain and practice an incident response plan to rapidly respond to a compromise • Review written security policies and procedures to ensure they contain the minimum guidance addressed above
Frameworks and Guidance	CISA CPGs 1.3, 1.5, 4.3, 7.1, 7.2 CIS Control 9 NIST CSF *PR.AC-5, DE.CM-4 & 7*
CISA Resources and Services	CISA Cross-Sector Cybersecurity Performance Goals Avoiding Social Engineering and Phishing Attacks Enhance Email & Web Security Cyber Hygiene Services

	Stop Ransomware | CISA Multi-Factor Authentication

Table 2: Vulnerable VPN Devices Scenario

Organizations implement virtual private networks (VPNs) to protect communications containing sensitive information. As described in the CRS, 3 of the 11 most prevalent Known Exploitable Vulnerabilities (KEV) were related to VPN vulnerabilities. Utilizing a VPN with vulnerabilities increases exposure to a multitude of attacks that threaten the confidentiality, integrity, and authenticity of sensitive data.	
Intended Target	VPN servers and data in transit
Complexity to Exploit	Complexity varies based on the vulnerability prerequisites needed to exploit
Method of Attack	• Directory traversal • Crafted HTTP requests • Heap buffer overflows • Cross-site scripting
Threat actor gain	• Arbitrary code execution • Authentication bypass • Remote file access • DOS capabilities

Mitigation Recommendations	• Document and implement a consolidated security policy for VPN systems
	• Ensure VPNs are configured correctly, patched regularly, and scanned on a consistent basis as outlined in NIST SP 800-113
	  ○ When possible, configure VPN abstractions at higher levels than network routing (e.g., Socket Secure (SOCKS) proxy)
	  ○ Ensure equal attention between client and server-side VPN assets
	  ○ Be sure to remove old protocols, such as point-to-point tunneling, from service if still in use
	• Harden VPN to reduce the VPN server's attack surface through:
	  ○ Configuring strong cryptographic authentication
	  ○ Running only strictly necessary features
	  ○ Protecting and monitoring access to and from the VPN

	When possible, restrict VPN access of endpoints using an IP allowlist • Place VPNs within your network's demilitarized zone (DMZ) and monitor them regularly • Operate VPNs in active/active mode to allow patching with minimal downtime • Regularly audit VPN user and permissions list • Enable MFA on all VPN access points • Consider FIDO authentication for VPN connections if available • Carefully select remote access VPNs from trusted and reputable vendors
Frameworks and Guidance	CISA CPGs 1.3, 8.1 CIS Controls 1, 2, 4, 5, 6, 7, 12, 13, 15, 18 NIST CSF ID.AM, ID.RA, ID.SC, PR.AC, PR.DS, PR.IP, PR.MA, PR.PT, DE.CM, DM.DP
CISA Resources and Services	CISA Cross-Sector Cybersecurity Performance Goals BOD 22-01-Reducing the Significant Risk of Known Exploited Vulnerabilities Known Exploited Vulnerabilities Catalog Cyber Hygiene Services

Table 3: Web Application Weakness Scenario

Web application vulnerabilities arise from a weakness or misconfiguration in the design or deployment of the application. Exposing web applications with known vulnerabilities provides threat actors with opportunities for malicious action.	
Intended Target	Applications, servers, and end users
Complexity to Exploit	Exploiting web application weaknesses varies from easy to sophisticated, based on the exploit available
Method of Attack	• Cross-site scripting (XSS) • SQL injection • Session replay attacks • Path traversal • Buffer overflow • Remote code execution • Local file inclusion • Distributed Denial of Service (DDOS) • Compromise of weak cryptographic algorithms • XML external entity (XXE) injection
Threat actor gain	• Access to sensitive organizational data • Credential acquisition • Account takeover fraud

	• Remote code execution • Disruption of functionality/business processes

Mitigation Recommendations	• Conduct in-depth security testing of web applications and servers prior to installing on the network
	• Utilize a web application vulnerability scanning service, such as CISA's Cyber Hygiene Services, to identify vulnerabilities before they can be exploited
	Common web application weaknesses include:
	• Broken Access control
	  ○ Except for publicly available data resources, deny access by default
	  ○ Log access control failures and alert administrators when appropriate (for example, repeated failures to access the application should be reported to the appropriate personnel)
	• Cryptographic Failure
	  ○ Classify data processed, stored, or transmitted by an application and implement additional security controls based on data classification
	  ○ Do not store sensitive data unnecessarily and ensure data at rest is encrypted
	  ○ Encrypt all data in transit with secure protocols such as TLS with forward secrecy (FS) ciphers, cipher prioritization by the server, and secure parameters
	  ○ Avoid using weak cryptographic algorithms such as MD2, MD4 and MD5 and RC4
	• Injection attack vulnerabilities
	  ○ Utilize a safe API, that avoids using an interpreter entirely, and provides a parameterized interface, or migrates to Object Relational Mapping Tools
	  ○ Use positive server-side input validation
	  ○ Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection
	• Insecure Design

	○ Use threat modeling for critical authentication, access control, business logic, and key flows ○ Limit resource consumption by user or service • Security Misconfigurations ○ Ensure all software is up to date and patches are implemented when available. ○ Disable unnecessary ports, protocols, and services • Vulnerable and outdated components ○ Remove unnecessary components, files, and dependencies ○ Only obtain components from reputable and official sources ○ Create and maintain software and hardware inventory lists that include versioning, and location • Identification and Authentication failures ○ Follow the National Institute of Standards and Technology (NIST) Special Publication 800-63b for password rotation, complexity, and rotation requirements ○ If incorrect passwords or usernames are given to the application, ensure the application gives a standard response for the access failure ▪ There should be no delineation between which field had invalid input • Data and Software integrity failures ○ Consider hosting an internal repository that has been vetted and is trusted ○ Utilize digital signatures or similar mechanisms such as comparing checksums to verify the integrity of the software or data ○ Implement and enforce a process for code and configuration changes • Security logging and monitoring failures

	○ Ensure auditable events such as login failures or transactions of critical data are actively logged and monitored ○ Harden logging and monitoring systems from attacks by ensuring log data is properly encoded ○ Ensure warning messages and errors generate easy to understand log messages for DevSecOps personnel • Server-Side Request Forgery ○ Disable HTTP redirects ○ Network firewall policies should deny unapproved traffic by default ○ Sanitize and validate all user supplied input data at the application layer
Frameworks and Guidance	CISA CPGs 1.1, 2.3, 3.1, 3.3, 5.1 CIS Controls 6, 7, 8, 9, 16 NIST CSF ID.AM-2, PR.AC
CISA Resources and Services	CISA Cross-Sector Cybersecurity Performance Goals BOD 22-01-Reducing the Significant Risk of Known Exploited Vulnerabilities Known Exploited Vulnerabilities Catalog Cyber Hygiene Services

Table 4: Utilization of Vulnerable Services Scenario

CISA considers services commonly targeted by threat actors to gain remote access to victim networks as vulnerable. Vulnerable services include any remote management services, services intended for use over a trusted network, and additional services that allow for potentially risky interaction. Although an organization may require some of these services for legitimate business needs, exposure introduces additional risk.	
Intended Target	Any asset exposing the vulnerable service
Complexity to Exploit	Complexity varies based on the vulnerable service that is being exploited.
Method of Attack	• SMB Relay attacks • Directory Traversal Attack • Anonymous FTP exploitation • NBTSTAT footprinting • Man-in-the-middle attack • SQL truncation attack • SQL injection attack • SQL Server registry manipulation • Credentialed access through brute force attacks and/or valid accounts

Threat actor gain	• System access from valid account acquisition • Unauthorized access to organizational network, sensitive data, and the exposed device
Mitigation Recommendations	• Minimize network exposure to only those services required by business need • Implement network segmentation to separate and restrict communications between publicly exposed endpoints and the internal network • Maintain updated versions of exposed services and remove support for outdated versions • Protect the exposure of vulnerable services by business need by requiring access by MFA through a VPN. Consider exposing the service on a nonstandard port to minimize ease of detection by threat actors through basic scanning techniques • Ensure Signature based Intrusion detection systems have their signature sets updated regularly • Undergo penetration tests to evaluate the effectiveness of current mitigating controls • Revoke "execute" function on dangerous SQL server functions • Identify essential SQL statements and include them in an allowlist ○ Ensure unvalidated statements are not included within your "allowed" statements • Define SQL code with prepared statements, to differentiate between code and user input • Ensure up-to-date notification agreements with third-party vendors are completed
Frameworks and Guidance	CISA CPGs 1.3, 2.1, 5.1, 5.4, 5.5, 5.6, 8.1 CIS Controls 1, 2, 4, 5, 6, 7, 8, 10, 12, 13, 18 NIST CSF DE.AE, DE.CM, PR.AC-5, PR.IP-12
CISA Resources and Services	CISA Cross-Sector Cybersecurity Performance Goals BOD 22-01-Reducing the Significant Risk of Known Exploited Vulnerabilities Known Exploited Vulnerabilities Catalog Cyber Hygiene Services

Table 5: Insecure Encryption Protocols Scenario

Organizations utilize encryption protocols to protect sensitive information in transit. If allowed to become outdated, the protocols' ability to provide this protection is compromised. Within the SLTT CRS the most prevalent high severity vulnerability detected was an insecure protocol—primarily the use of deprecated SSL versions within stakeholder environments. Utilizing weak or outdated encryption protocols is typically indicative of poor cyber hygiene practices and is often observed in conjunction with other vulnerabilities, inviting threat actors to further attempt to locate and exploit weaknesses.	
Intended Target	Any data in transit utilizing insecure encryption protocols
Complexity to Exploit	Exploiting weaknesses within insecure encryption protocols requires very few skills and is dependent upon the threat actor's ability to meet attack prerequisites and circumvent mitigating controls in place
Method of Attack	• Man-in-the-middle attacks • Downgrade attacks • Replay attacks • Known plaintext attack • Chosen plaintext attack • Cipher-only attack
Threat actor gain	• Access to decrypted information

Mitigation Recommendations	• Avoid using weak ciphers (e.g., MD4, MD5, RC4, RC2, DES, Blowfish, SHA-1)
	• Disable outdated or insecure protocols (e.g., SSL, TLS 1.0, TLS 1.1)
	  ○ Opt-in for the latest SSL/TLS protocol
	  ▪ TLS 1.2 or 1.3
	• Maintain awareness of current protocols and configure within your servers to enable the most current version
	• Maintain updated and properly registered TLS/SSL certificates
	  ○ Ensure certificate authority is valid (or trusted)
	• Consult vendor guidance to configure secure encryption protocols
	• Conduct on-going SSL/TLS web application vulnerability scanning

Frameworks and Guidance	CISA CPG 3.3 CIS Controls 3, 4, 7 NIST SP 800-52 Rev. 2
CISA Resources and Services	CISA Cross-Sector Cybersecurity Performance Goals

	BOD 22-01-Reducing the Significant Risk of Known Exploited Vulnerabilities Known Exploited Vulnerabilities Catalog Cyber Hygiene Services

Conclusion

By following the defensive mitigation strategies detailed in this document, SLTT governments can work to significantly reduce their cybersecurity risk. Priorities for SLTT governments should include: (1) minimizing the success of phishing campaigns, (2) ensuring your networks are segmented to reduce your attack surface, and (3) implementing a robust patch management program to reduce the likelihood of vulnerability exploitation. This supplement, along with the SLTT Government Facilities Sector Cyber Risk Summary, encourages SLTT governments to implement mitigations and best practices necessary to protect their IT and OT infrastructure.

Feedback regarding this product is critical to CISA's continuous improvement. If you have feedback specific to your experience with this product, please send CISA your input by filling out the CISA Product Survey.

Appendix A – Abbreviations

Acronym	Meaning
API	Application Programming Interface
AV	Antivirus
BOD	Binding Operational Directive
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CRS	Cyber Risk Summary
CSF	Cybersecurity Framework
DMZ	Demilitarized Zone
DoS	Denial of Service
EDR	Endpoint Detection and Response
FIDO	Fast IDentity Online
FS	Forward Secrecy
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IT	Information Technology
KEV	Known Exploited Vulnerabilities
MFA	Multi-Factor Authentication
NBTSTAT	NETBIOS Over TCP/IP Statistics
NIST	National Institute of Standards and Technology
OT	Operational Technology
PhaaS	Phishing as a Service
SLTT	State, Local, Tribal, Territorial
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network
XSS	Cross-Site Scripting

Appendix B – Relevant Terms

Term	Definition
Attack Surface	The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.
Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
Endpoint	A remote computing device that communicates back and forth with a network to which it is connected.
Footprinting	The process of collecting information about a target network and its environment.
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Likelihood	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Appendix C – Embedded Resources

Organization	Links
CISA	• Cross-Sector Cybersecurity Performance Goals • Cross-Sector Baseline Cybersecurity Performance Goals (CPGs) • Cybersecurity Training & Exercises | CISA • Report Phishing Sites | CISA • Zero Trust Maturity Model | CISA • New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks | CISA • Cyber Hygiene Web Application Scanning | CISA • CISA Publishes Infographic on Layering Network Security Through Segmentation | CISA • Avoiding Social Engineering and Phishing Attacks • Vulnerability Assessment (RVA) and Phishing Campaign Assessment (PCA) • Stop Ransomware | CISA • Enhance Email & Web Security • BOD 22-01-Reducing the Significant Risk of Known Exploited Vulnerabilities • Known Exploited Vulnerabilities Catalog • Cyber Hygiene Services • Multi-Factor Authentication • Selecting and Hardening Remote Access VPN Solutions • Security Tip (ST05-010) Understanding Website Certificates
CIS	• CIS Critical Security Controls • CIS Benchmarks
OWASP	• A01 Broken Access Control - OWASP Top 10:2021 • OWASP Top Ten Proactive Controls 2018 | C7: Enforce Access Controls | OWASP Foundation • A02 Cryptographic Failures - OWASP Top 10:2021 • OWASP Top Ten Proactive Controls 2018 | C8: Protect Data Everywhere | OWASP Foundation • WSTG - Latest | OWASP Foundation • A03 Injection - OWASP Top 10:2021 • A04 Insecure Design - OWASP Top 10:2021

Organization	Links
	• A05 Security Misconfiguration - OWASP Top 10:2021 • A06 Vulnerable and Outdated Components - OWASP Top 10:2021 • OWASP Dependency-Check | OWASP Foundation • A07 Identification and Authentication Failures - OWASP Top 10:2021 • A08 Software and Data Integrity Failures - OWASP Top 10:2021 • A09 Security Logging and Monitoring Failures - OWASP Top 10:2021 • Logging - OWASP Cheat Sheet Series • A10 Server Side Request Forgery (SSRF) - OWASP Top 10:2021 • Input Validation - OWASP Cheat Sheet Series
Microsoft	• How to implement Multi-Factor Authentication (MFA) - Microsoft Security Blog • REVOKE Object Permissions (Transact-SQL) - SQL Server | Microsoft Docs • About Highly Available gateway configurations - Azure VPN Gateway | Microsoft Docs
GitHub	• SSL and TLS Deployment Best Practices · ssllabs/research Wiki · GitHub • Encoding and escaping untrusted data to prevent injection attacks | The GitHub Blog
AT&T	• 2021 Email Server Security Best Practices | AT&T Cybersecurity (att.com) • 2021 Intrusion Detection Techniques, Methods & Best Practices | AT&T Cybersecurity (att.com)
MITRE	• CWE - CWE-20: Improper Input Validation (4.8) (mitre.org)
Threat Modeling Manifesto	• Threat Modeling Manifesto
Rapid7	• What is Patch Management? Benefits & Best Practices | Rapid7
True Digital	• A Better Way to Manage Your Software Inventory | True Digital Security

Organization	Links
NIST	• SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Mgmt | CSRC (nist.gov) • SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations • Guide to SSL VPNs | NIST • Framework for Improving Critical Infrastructure Cybersecurity • Back to basics: Multifactor authentication (MFA) | NIST
CISCO	• What is Penetration Testing? - Pen Testing - Cisco
Geeks for Geeks	• Basic SQL Injection and Mitigation with Example - GeeksforGeeks
Red Canary	• How to Implement an EDR Capability in Your Security Program (redcanary.com)