SEC-11-02-S
State CIO Adopted: August 11, 2023
TSB Approved: September 14, 2023
Sunset Review: September 14, 2026

Replaces:
IT Security Standard 141.10 (5.5 & 5.6)
December 11, 2017

WaTech
Washington Technology Solutions

VULNERABILITY MANAGEMENT STANDARD

See Also:
RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"
RCW 43.105.450 (7c) IT Security
NIST SP 800-40 Guide to Enterprise Patch Management Planning

1. Vulnerability scanning must include the following activities:

a. All computing and networking IT assets identified by the Asset Management Policy must be included in the vulnerability assessment scope.

b. Configure endpoints and network infrastructure and applications to allow access for vulnerability scans.

c. Schedule and conduct monthly scans of internal-facing computing and networking IT assets.

d. Schedule and conduct weekly scans of internet-facing computing and networking IT assets.

e. Perform vulnerability scans after the introduction of new computing or network devices into the agency IT environment.

f. Verify all findings identified during the vulnerability scan and document supporting evidence. The following types of evidence may suffice for documentation of a False Positive:

i. Narrative with a screenshot showing that the information provided is incorrect.

ii. Any other items that would indicate that the information provided is inaccurate.

2. Agencies must prioritize the vulnerabilities they will address.

a. Agencies must prioritize the assets to be remediated by the system's business criticality.

b. Agencies must triage vulnerabilities listed in the Known Exploited Vulnerabilities (KEV) Catalog for remediation.

c. Agencies must use the highest vulnerability criticality from the Vulnerability Management Procedure or the Common Vulnerability Scoring System (CVSS) ratings in Table 1 to triage vulnerabilities not listed in the KEV Catalog.

Table 1 – Vulnerability Classification

Vulnerability Classification	Description	CVSS Rating
Critical	Indicates flaws could be easily exploited by an unauthenticated remote attacker and lead to compromise.	9.0 – 10.0
High	Indicates local users can gain privileges, allow unauthenticated, remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service.	7.0 – 8.9
Medium	Indicates flaws are more difficult to exploit but could still lead to compromise under certain circumstances.	4.0 – 6.9
Low	Indicates vulnerabilities require unlikely circumstances to be exploited or where a successful exploit would cause either no adverse effect or result in minimal adverse consequences.	Below 4.0
Informational	Useful information that is more general about the system and how it operates. Mostly configuration choices rather than a real vulnerability.	0

d. Agencies must prioritize based on the risk assessed. See the Risk Assessment Standard.

   i. Agencies prioritizing their remediation workload must consider existing network, IT system, and/or application security layers that may reduce the likelihood and/or impact of a vulnerability.

   ii. Agencies must track backlogs of pending remediations.

e. Identify a vulnerability mitigation plan for assets for which no patch is available.

3. **After confirming the vulnerability scan results applicable to their systems, agencies are responsible for reducing the likelihood and/or the impact of exploitation of the vulnerabilities.**

   a. Agencies must mitigate the vulnerability using vendor security patches, system configuration changes and/or application modifications, and other appropriate mitigation strategies. All changes must be documented per the agency's change management processes.

   b. Agencies will reference the Common Vulnerability and Exposure (CVE) database.

   c. Agencies will take the necessary corrective actions. The corrective actions recommended in the vulnerability scanner and reports are to be used as a guideline for mitigation strategy.

   d. Agencies must verify the successful application of vulnerability patches. If the confirmation scan reveals that the mitigation was unsuccessful, further action must be taken to remediate the vulnerability.

   e. If a recommended remediation step is not possible, agencies must develop and implement compensating controls.

   f. The compensating controls will operate until vendor patches or configuration changes are available.

   g. If the vulnerability cannot be patched, agencies must harden the affected IT asset according to the Configuration Management Standard to reduce the likelihood of vulnerability exploitation.

4. **Agencies must maintain a documented patch management procedure for all computing and network assets under their control. The procedure must include the following steps at a minimum:**

    a. Identification and prioritization of patches to be installed.

    b. Applying patches in a timeline consistent with business criticality and risk.

    c. Coordination of a patch window with appropriate stakeholders.

    d. Validation of the appropriate application of patches.

    e. Evaluation and testing of patches prior to deployment.

    f. Agencies must install patches that address previously unknown exploits (Zero-Day Exploit) with a critical CVSS and high risk assessed within one calendar day of patch release.

    g. Agencies unable to meet their established deadlines for patching vulnerabilities with high CVSS scores for high-risk systems as assessed by the agency must identify and document compensating controls and notify WaTech by filing a ServiceNow ticket.

5. **Agencies must conduct ongoing external threat intelligence gathering, which at a minimum includes identification and use of threat intelligence feeds.**

6. **Agencies must document their vulnerability management plan based on the requirements in this standard. The vulnerability management plan must include:**

    a. A list of the vulnerabilities to be patched, including the CVSS severity ranking in Table 1.

    b. Mean time to remediate.

    c. The computing and network IT assets the agency did not remediate.

REFERENCES

1. Definitions of Terms Used in WaTech Policies and Reports
2. Asset Management Policy
3. Known Exploited Vulnerabilities Catalog | CISA
4. Common Vulnerability Scoring System (CVSS)
5. Configuration Management Standard
6. Risk Assessment Standard
7. Vulnerability Management Procedure (under development – will be

confidential due to security)

8. Common Vulnerability and Exposure (CVE) database

9. NIST Cybersecurity Framework Mapping:

   Identify.Risk Assessment-1 (ID.RA-1): Asset vulnerabilities are identified and documented.

   Protect.Information Protection Processes and Procedures-12 (PR.IP-12): A vulnerability management plan is developed and implemented.

   Detect.Security Continuous Monitoring-8 (DE.CM-8): Vulnerability scans are performed.

   Respond.Analysis-5 (RS.AN-5): Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).

   Respond.Mitigation-3 (RS.MI-3): Newly identified vulnerabilities are mitigated or documented as accepted risks.

CONTACT INFORMATION

- **For questions about this policy, please contact the WaTech Policy Mailbox.**
- **To request a Security Design Review, please contact the Security Design Review Mailbox.**