UNT | SYSTEM™

Vulnerability Management Standards
Information Security

Overview

Custodians must manage system vulnerabilities to minimize risk and protect information systems from exploitation and targeted attacks.

The Vulnerability Management Program Standard, along with the policies in the UNT System Information Security Handbook, provides guidance for custodians responsible for the security of computer systems. This standard presents guidance regarding sources of vulnerability information, vulnerability assessment frequency, vulnerability remediation timelines, and vulnerability exception requirements.

Vulnerabilities that are remediated manually, i.e., remediation is not automated, must undergo an assessment and approval process that includes the following:

- Identification of the vulnerability
- Conduct a risk assessment that identifies the impact and likelihood of the consequences that may occur if the vulnerability is not remediated. The risk assessment should include a technical and business impact assessment.
- Identify the urgency (priority) involved in remediating the vulnerability
- Remediation actions must be tested prior to placing asset into production and after placing asset into production to ensure that results occur as expected
- Follow change management process including stakeholder approval
- Obtain approval from stakeholders prior to placing asset into production after remediation has occurred as required by change management process
- Assessment and remediation must be documented

Sources and Monitoring for Vulnerability Identification

- Rapid7 InsightVM
    - The Insight Agent provides continuous monitoring
    - Monthly network discovery scans
        - Information Security will perform monthly discovery scans to identify network assets where no agent is present and conduct network assessments when appropriate
        - Information Security and custodians will identify critical assets not running Insight agent and contact responsible administrator requesting installation
- Vendor Website
    - Vulnerability disclosures
    - Patch notes
    - Configuration recommendations
- Third-party disclosure
    - Independent security researchers

Risk Assessment and Testing

- Custodians must track and document all assets within their area of responsibility.
- InsightVM will be used to conduct vulnerability risk assessments on devices with the agent installed.
- Vulnerability assessments must be conducted throughout the lifecycle of an asset. Assessments must occur during development of the asset, during testing, prior to placing the asset into production, and regularly after an asset has been deployed.
- Vulnerabilities must be remediated prior moving or placing an asset into production.
- Assets must be tested prior to being placed into production to determine if vulnerability assessment tools can be used to scan the asset for vulnerabilities.
- Risk assessments must be conducted that identify the impact and likelihood of the consequences that may occur if a vulnerability is not remediated. Risk assessments should be conducted as follows:
    - Prior to updating high impact systems and assets
    - Risk assessments must consider the likelihood of success and the impact to the affected service
    - Risk assessments are recommended for systems and assets with medium criticality
    - Systems and assets with low criticality are not required to undergo a risk assessment
    - Systems or assets with vulnerabilities associated with low CVSS/CVE severity scores are not required to undergo the risk assessment process
- End-of-life assets are information resources that have reached date in which the resources are no longer capable of being patched, updated, or receiving technical support that ensures the security of the asset. End-of-Life systems have been identified by the manufacturer as being no longer viable for continued use. End-of-Life assets should be removed from the network and their use should be discontinued. In cases where end-of-life systems must remain operational a risk assessment must be conducted and compensating controls must be utilized and documented. In addition, the asset must undergo the security exception process. Requests for security exceptions must be directed to the office of the Chief Information Security Officer.

Triage and Remediation Priority

- Custodians must remediate vulnerabilities within set timeframes that are based on the criticality of the asset that they are responsible for administering and the severity of a vulnerability associated with an asset. See "Remediation Timeframes by Severity Rating and System Criticality" chart below for allowable timeframes.

Remediation Timeframes by Severity Rating and System Criticality Table

	System Criticality High/Critical	**System Criticality Medium**	**System Criticality Low**
Actively Exploited Vulnerabilities	ASAP	ASAP	ASAP
CVSS High/Critical 7.0-10	Patched ASAP. No later than 30 days.	Patched ASAP. No later than 30 days.	Patched ASAP. No later than 30 days.
CVSS Medium 4.0-6.9	Patched ASAP. No later than 90 days.	Address during regular system maintenance cycle. No later than 180 days.	Address during regular system maintenance cycle. No later than 180 days.
CVSS Low 0-3.9	Address during regular system maintenance cycle. No later than 180 days.	Address during regular system maintenance cycle. No later than 180 days.	Address during regular system maintenance cycle. No later than 180 days.

- Custodians must triage and remediate vulnerabilities on critical primary and secondary systems whether or not InsightVM can monitor or assess the systems.
- Devices with unmitigated risk are subject to removal from the network and may be decommissioned.
- Information Security will report to management any vulnerabilities that custodians do not remediate within the timeframes specified in the Severity Rating / Criticality Matrix.
- Remediation Options
  - Patching and Updating– Automatic patching and updating are the easiest and most common method for remediating a vulnerability.
  - Configuration changes – Configuration changes are workarounds to patching and can be implemented when patching is not an option.
  - Compensating controls – Compensating controls can be utilized as temporary control until a patch is applied and may also be the sole remediation option when other remediation choices are deemed not suitable. Compensating controls include air-gapping or implementing firewalls and other changes that reduce the impact of a vulnerability. Compensating controls must be documented and approved.
  - Upgrade - Where applicable, assets can be upgraded to new platforms to ensure vulnerabilities are addressed.
  - Migrate - Where applicable, assets can be migrated to new platforms to address vulnerabilities
  - Vulnerability remediation efforts must follow change management standards.
  - Risk acceptance

- Whenever a vulnerability is not remediated, either indefinitely or for a short time, the organization is accepting the associated risk. This is not a recommended option. There are unique occasions that an organization will choose to accept the risk of leaving the vulnerability open. Contact the Chief Information Security Officer for a security risk review and to obtain approval for a security exception.
- Per the Handbook, section 20. General Security Exceptions, “The Information Security Officer will coordinate exceptions and compensating controls with information and service owners. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process. The Information Security Officer will provide an approval or rejection of a request for security exception to the custodial department. The Information Security Officer may revoke security exceptions at any time.”

- Vulnerability exceptions for false positives
    - Custodians can submit a support ticket in ServiceNow for suspected false positives in the vulnerability assessment tool
    - Any request for an exception other than false positive reporting must undergo the standard security exception process and must be approved by the Information Security Officer.

References

UNT System Information Security Handbook, (see section 14.5 Vulnerability Management)
https://itss.untsystem.edu/divisions/mrs/is/unt-system-information-security-handbook

Texas Department of Information Resources Security Control Standards Catalog
http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog.pdf

IT Change Management Standard

Document Version Log

Version	Date	Description
1.0	8/12/2021	Initial Document Version
1.1	9/15/2021	Document approved