Draft

Vulnerability Management Guidelines

Purpose

The purpose of vulnerability management is to prevent the exploitation of known vulnerabilities. Vulnerabilities can be due to software bugs that can be exploited for malicious purposes, as well as insecure system configurations and settings, such as weak or default passwords. These guidelines establish a framework for identifying and remediating vulnerabilities to minimize security breaches.

Scope

These guidelines apply to desktop systems, network devices and computer servers attached to the University network.

Patch Management

Patch management is a key element of vulnerability management. Vendors regularly issue security updates to fix known vulnerabilities. To maintain the security of operating systems and application software, security patches must be installed and kept up to date.

The following are guidelines for applying security patches:

- Security patches for exploits in the wild should be patched within 48 hours of publication.
- Security related updates should be applied within 5 business days of release.
- Systems and software should be patched at least quarterly with routine updates.
- Where systems can not be patched due to negative impact to business operations a Plan of Action & Milestones report will be presented to the appropriate ISO.
- Automated patch management tools are available through the Office of Information Technology. For information, contact the OIT Support Center.

Vulnerability Scanning

Scanning systems for known vulnerabilities helps to identify where vulnerabilities exist. It also helps to validate that security patches are being applied.

The following are guidelines for performing vulnerability scans.

- Systems/devices connected to UA managed networks should be scanned for vulnerabilities monthly.

- Vulnerabilities found should be remediated in a timely manner based on severity. The table below provides a suggested remediation schedule. The severity classifications are based on the Common Vulnerability Scoring System (CVSS) and are defined by the NIST National Vulnerability Database.

Severity	**Description**	**Remediation Schedule**
Critical		
High		
Medium		
Low		
Informational		

- To ensure that scans are comprehensive and accurate, they should be performed with Administrator level privileges.

- Before a new server is put into production, it should be scanned for vulnerabilities. Critical, Severe or Medium vulnerabilities should be remediated and the server rescanned to verify the vulnerability has been resolved before it is operational. Exceptions can be made, such as a server needing to be brought online in the event of an emergency, however, a follow up scan should be performed and any problems found should be remediated in a timely manner.

- The Office of Information Technology will perform periodic scans of systems on the University network. In most cases attempts will be made to notify the system administrators or their managers in advance of the scans, however, there may be some situations where advance notification is not possible. Results of scans will be provided for follow up remediation. Departments can also request routine scans of their systems. Several options are available. For more information, contact the OIT Support Center.

Security Advisories

Information on security updates are available from a number of sources including directly from software vendors. System and application administrators are expected to monitor these lists and stay informed of when security updates are available for operating systems and applications they are responsible for maintaining. Several major sources are listed below: