CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Vulnerability Management Standard

CSUSB, Information Security &
Emerging Technologies Office

Last Revised: **09/17/2015**

Final

REVISION CONTROL

Document Title: CSUSB Vulnerability Management Standard

Author: Javier Torner

File Reference:

Date	By	Action	Pages
09/15/2015	J Torner/J Macdonell	Created document.	All
9/17/2015	L Carrizales	Standard approved by ISET Subcommittee on 9/16/15. Made changes to the document based on recommendations from ISET Subcommittee.	All

Review/Approval History

Date	By	Action	Pages
9/16/2015	ISET Subcommittee	Approved standard.	All

Contents

Vulnerability Management Standard

1. Introduction

An essential component of risk management for information technology (IT) infrastructure is the inventory and remediation of known vulnerabilities.

Vulnerabilities pose a risk to the confidentiality, integrity, and availability of University resources, as well as those whose data is stored by the University, or others that access University systems. To reduce this risk, vulnerabilities should be inventoried and remediated in a timely manner.

Specific techniques for inventory and remediation are specified in the CSUSB Vulnerability Management Guidelines.

2. Scope

This standard applies to all IT systems, IT applications, and repositories of sensitive information, including paper repositories of sensitive information. Examples include, but are not limited to: servers, workstations, network appliances, cameras, printers, multifunction copiers, vendor-maintained systems, and third-party as-a-service applications.

Highest priority is directed to Internet-facing systems that interact with Level 1 or large quantities of Level 2 classified information.

Then, workstations and other non-Internet-facing (intranet) systems that interact with Level 1 or large quantities of Level 2 classified information.

Then, laptops and mobile devices that interact with Level 1 or large quantities of Level 2 classified information.

Then, off-line repositories of sensitive information, including paper repositories

Then, Internet-facing systems with Level 3 classified information

Then, non-Internet-facing systems with Level 3 classified information, including workstations, laptops, mobile devices, printers, appliances, etc.

Then, off-line systems

3. Roles & Responsibilities

3.1. Information Security and Emerging Technologies (ISET Office):

- Develop and maintain vulnerability management documentation and training
- Provide delegated access to vulnerability inventory (scanning or similar) resources to system owners and application developers.
- Monitor compliance with this standard
- Identify non-compliant systems and contact system owners and business area administrators prior to quarantine or isolation from campus network.

3.2. Telecommunications and Network Services

- Isolate non-compliant systems and applications from campus network

3.3. System and Application Owners

- Register servers and applications in credentialed vulnerability scanner.
- Configure servers and applications for appropriate authenticated vulnerability scans (coordinated with ISET Office).
- Perform vulnerability scans and remediate any Medium or higher severity vulnerabilities prior to moving application into production.
- Schedule on-going vulnerability scans.
- Review and validate periodic vulnerability scan reports.
- Mitigate vulnerabilities within the required mitigation schedule.

3.4. Separation of Duties

- System administrators and developers may perform preliminary or on-demand unofficial scans.
- To gain access to the scanning tool, send an email to security@infosec.csusb.edu.

4. Vulnerability Inventory

4.1. Techniques

Inventory of network connected assets is typically conducted using scanning tools as specified in the CSUSB Vulnerability Management Guidelines.

Some information assets, such a paper repositories, require other techniques, such as a physical security inventory using a tool such as the sensitive data questionnaire.

4.2. Scanning Tools

CSUSB's ISET Office is responsible for overseeing and delegating campus use of enterprise vulnerability scanning and assessment tools. Use of enterprise tools is preferred to facilitate consistent university-wide metrics and reporting.

Using another vulnerability scanning tool in lieu of the enterprise tools may be acceptable, pending approval from the ISET Office. The other tool should be similar in functionality to the enterprise tools and capable of exporting reports compatible with the enterprise tools.

Use of any complementary tools is encouraged. Suggestions for tools to be used enterprise-wide are appreciated and should be forwarded to the ISET Office.

4.3. Scanning Scope

Scanning tools are intended to be used against systems and applications connected to the CSUSB network (on-campus).

Servers (e.g. infrastructure-as-a-service) or applications (various other -as-a-service offerings) hosted outside the CSUSB network (off-campus) are in scope of this standard. However, CSUSB will give hosting providers a 72 hour notice of intent to conduct scanning to allow time for the provider to accommodate the scan or otherwise object. Pending approval by the ISET Office, other options may be used instead, such as: vulnerability scanning agents, vendor-reported vulnerability scans, or contractual language.

4.4. Frequency - Scanning

4.4.1. Lifecycle Events

Vulnerability scans are conducted in conjunction with significant system or application lifecycle events, such as promotion from staging to production.

If medium-risk or higher vulnerabilities are discovered, they are remediated before the system is placed into production. A follow up scan is conducted to confirm the system is cleared of medium-risk or higher vulnerabilities.

4.4.2. Periodic

All campus servers, prioritized by scope, are scanned using authentication at least quarterly. This focuses on the operating system and other installed software. Systems interacting with Level 1 or large quantities of Level 2 data should scan weekly.

All applications, prioritized by scope, are scanned for vulnerabilities at least once a quarter using an application aware scanning configuration. Systems interacting with Level 1 or large quantities of Level 2 data should be scanned weekly wherever automated scans are applicable.

4.5. Frequency - Other techniques

For information assets and repositories where a network vulnerability scan is inappropriate, such as a paper repository, a yearly physical vulnerability inventory must be conducted using a tool similar to the sensitive data questionnaire.

5. Vulnerability Remediation

There are several options for remediating a vulnerability. These are described further in the CSUSB Vulnerability Management Guidelines. Options include:

- Apply patch or update
- Implement a documented work-around
- Determine that the issue is a false positive
- Determine that the issue can be reclassified or mitigated
- Obtain a waiver or extension

5.1. Timelines and Prioritization

Vulnerability scan reports typically classify vulnerabilities found. The most common classifications are:

- CRITICAL
- HIGH
- MEDIUM
- LOW
- INFORMATIONAL

Various tools may also use terms Urgent for Critical and Serious for High. Additionally the Common Vulnerability Scoring System (CVSS) may be used. Per NIST standard, CVSS base scores in the range 7.0-10.0 are considered as High (although 9.0-10.0 should be considered Critical), those in the range 4.0-6.9 as Medium, and 0-3.9 as Low.

The following timelines must be followed when remediating vulnerabilities to avoid a system or application being classified as non-compliant. The table list the maximum amount of time between a vulnerability inventory and remediation.

Critical severity	24-48 hours
High severity	Four weeks
Medium severity	Six weeks

5.2. Enforcement

Systems and applications not remediated within the standard remediation schedule or timeframe are classified as non-compliant and will be quarantined. Under normal circumstances, non-compliant server and application owners and their respective administrative departments will be provided a warning 7 days from detection prior to removal from the network and quarantined. Incident handling procedures may take precedence.

5.3. Waivers and Extensions

The waiver or extension option exists for security issues that are a valid concern but cannot or will not be fixed within standard timelines for business or other reasons. A situation that would require an extension might include the critical processing freeze.

To avoid timeline enforcement, a waiver or extension request must be submitted to the issue tracking system including the rationale for the waiver or extension. The issue should then be reassigned to the ISET Office. The ISET Office will verify the rationale, and present the waiver to the Information Security Officer who, in collaboration with the appropriate MPP, develops a mitigation plan in support of the request. When the final decision is made, the ISET Office will update the waiver or extension status in the issue tracking system in addition to notifying the requester of the status. In the event of an extension, the extension expiration date should be documented in the issue tracking system. The issue tracking system case should be kept open until every issue has been resolved through something other than an extension request.

5.4. False Positives

If a discovered vulnerability is determined to be a False Positive, the finding, in addition to supporting rationale, must be documented in the issue tracking system. It must be documented before being automatically excluded from future inventories. False positives that are configured to be automatically excluded from inventory should be revalidated quarterly if a revalidation/expiration feature is present in the vulnerability scanning software.

5.5. Reclassification

In some cases, an inventory tool will flag a possible vulnerability that, upon examination, is confirmed to indeed be a vulnerability, but for business or other reasons the concern is not relevant in the specific situation. In such a situation, the security posture desired by CSUSB takes precedence over the security posture of the scanner and the vulnerability should be reclassified to a lower severity.

The finding, with supporting rationale, must be documented in the issue tracking system before being automatically reclassified in future inventories.   If a vulnerability is configured to be automatically reclassified, that process should be revalidated quarterly if a revalidation/expiration feature is present in the vulnerability scanning software.

5.6. Mitigation

Occasionally, a vulnerability is discovered for which no corrective action is available. In such cases, appropriate mitigating controls, such as limiting firewall access or requiring a second factor for authentication, must be implemented instead. Mitigated vulnerabilities that are configured to be automatically excluded from the inventory must be documented in the issue tracking system and reviewed by the ISET Office. Automatically excluded vulnerabilities should be revalidated quarterly if a revalidation/expiration feature is present in the vulnerability scanning software.

6. References

CSU Policy ICSUAM 8045.0 Information Technology Security
Policy Reference: http://www.calstate.edu/icsuam/sections/8000/8045.0.shtml

CSU Policy ICSUAM 8070.0 Information Systems Acquisition, Development and Maintenance
Policy Reference: http://www.calstate.edu/icsuam/sections/8000/8070.0.shtml

CSU Standard ICSUAM 8070.S000 Application Security Standard
Policy Reference:
http://www.calstate.edu/icsuam/sections/8000/8070.S000_Application_Security.pdf