SAN JOSÉ STATE UNIVERSITY

Standard: Vulnerability & Patch Management

Executive Summary

San Jose State University (SJSU) is highly diversified in the information that it collects and maintains on its community members. It is the university's responsibility to be a good steward and custodian of the information that it has been entrusted, which must be upheld by all members of the university. Per CSU Information Security Policy 8045.0 Section 500, San Jose State University (SJSU) is required to implement appropriate controls to monitor and scan network resources and information systems to identify and remediate vulnerabilities on networked computers. Proactively managing vulnerabilities can provide vital information to management and computer administrators of known and potential vulnerabilities for our organization to mitigate the vulnerabilities and improve SJSU's security risk posture. As a result, it could save the organization resources and time otherwise needed to respond to incidents after exploitation has occurred. Vulnerability Management and Assessment standard defines the requirements for vulnerability management and assessment for all SJSU computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed and transmitted by SJSU.

Information Security Standards

Vulnerability Management and Assessment

Standard #	IS-VMA	Effective Date	5/26/14	Email	security@sjsu.edu
Version	3.0	Contact	Information Security Officer	Phone	(408) 924-1530

Revision History

Date	Action
5/26/2014	Draft sent to ISO (Mike Cook)
12/1/2014	Reviewed. Updated. (Hien Huynh)
11/1/2020	Reviewed, updated with Remediation Matrix and Patching Policy. (Michael Hastings)

Table of Contents

Introduction and Purpose

This standard defines the requirements for vulnerability management and assessment for all San Jose State University (SJSU) computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by SJSU.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") computer systems and facilities, with a target audience of SJSU Information Technology employees and partners.

Standard

A standard for vulnerability management and assessment of network devices will be developed, and maintained by the Information Security Office (ISO).

Patch Management

Patch Management is the process of applying targeted changes to software programs, operating systems, or supporting data. The purpose of a patch is to either update the system to a newer version (as many older versions end up becoming unsupported eventually), or to supply code to fix an existing problem. Vulnerability patching is performed with the aim of fixing problems that could allow someone entry to your network or systems.

Vulnerability Management

Vulnerability management is designed to proactively mitigate or prevent the exploitation of technical vulnerabilities that exist in IT Resources. It is everyone's responsibility to maintain systems they hold direct ownership or control over to help keep SJSU's environment as safe and protected as possible. The following steps are a shared responsibility between the end user, system and application owners and administrators, Campus Techs, and the IT Security Office.

The Vulnerability Remediation process includes:

- Proactively scanning or identifying vulnerabilities;
- Investigating identified vulnerabilities;
- Assessing the severity and threat;
- Consulting with and informing appropriate individuals;
- Remediation; and
- Reporting.

Remediation may include one or more of the following:

- Patching or upgrading vulnerable software (the plan should include testing the patch/upgrade prior to deployment in production environment);
- Replacing the vulnerable software with a different product;
- Consolidating or moving to a more controlled environment;
- Changing the system configuration:
    - Disabling or turning off the vulnerable service
    - Disabling a specific vulnerable feature or capability within the service;
- The setting, changing or using a more complex password;
- Limiting access using a firewall or filter;
- Increase monitoring to detect anomalies;
- Documenting false positives;
- Informing users and management of the vulnerability.

Management of Technical Vulnerabilities

Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. Timely information about technical vulnerabilities of information systems being used should be obtained, the campus's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Remediation of Technical Vulnerabilities

Depending on the Severity of the vulnerability based on Qualys or RiskSense score reporting, the actions taken to remediate vulnerabilities should be carried out according to the SJSU Vulnerability Remediation Matrix. System and application upgrades should go through proper controls related to change management, or by following general University information Security Incident Response Procedures (e.g., isolate computer) and/or other escalation processes.

Patching Process

All systems must use approved patching application/process. Required patches for servers and endpoints must be installed every 30 days for routine updates, and ASAP for critical/emergency patches for vulnerabilities.

Vulnerability Advisories and Intelligence Feeds

On at least a weekly basis, systems administration staff must review all information security vulnerability advisories issued by trusted organizations for issues affecting campus systems. ISO and Administrators will subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis.

Periodic Vulnerability Scanning of Internal Network

Each campus IT department must run ISO approved automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.

Vulnerability Scanning of Internet Exposed Network

To ensure that SJSU technical staff has taken appropriate preventive measures, all systems directly-connected to the Internet must be subjected to an automated risk analysis performed via ISO approved vulnerability scanning software at least once a month.

Inventory of Production Software Versions

Each campus IT department must track and maintain a current inventory of all software used in production systems.

Security Advisory Patch Management

All security advisory patches for known vulnerabilities issued by a vendor must be promptly tested and installed within the time frame required by ISO.

On-Going Third Party Security Configuration Scanning

All SJSU computers accessible from the Internet, as well as all internal production computers, must be regularly scanned by a reputable third party security vulnerability scanning service.

Vulnerability Scanner supporting CVE and SCAP

The vulnerability scanner used by SJSU will support the identification of vulnerabilities based on CVE ID as well as SCAP configuration based vulnerabilities, where applicable.

Authenticated User Vulnerability Scanning

Vulnerability scanning should run in authenticated user mode, where applicable, with agents running locally on each end system to analyze the security configuration or with remote vulnerability scanners that are given administrative rights on the systems tested. A dedicated account for authenticated vulnerability scans should be used, with the account limited and used only for vulnerability testing.

References

CSU Information Security Policy -8045.0
Information Security Policy-Section 500 Information Asset Monitoring