CSUN INFORMATION TECHNOLOGY	Vulnerability Management Procedure For Websites and Web Applications February 16, 2017

Overview

This document clarifies the campus procedure for vulnerability management, including scanning, assessment, and remediation of the discovered vulnerabilities for CSUN websites and web applications. The results of the vulnerability scans inform web and application administrators of known and potential vulnerabilities, so those vulnerabilities can be remediated.

A vulnerability is a security exposure in an operating system or other system software or application software component including, but not limited to: missing operating system and application patches, inappropriately installed or active applications and services, software flaws and exploits, misconfigurations in systems, etc.

Related Polices and Standards

- CSU Information Security Policy - 8000.00 - Introduction and Scope
- CSU Information Security Policy - 8070.00 - Information Systems Acquisition, Development and Maintenance
- CSU Information Security Standard - 8070.S000 - Application Security

Vulnerability Assessment

No new website or new web application shall be migrated and considered to be in production until a vulnerability assessment has been conducted and vulnerabilities remediated.

Vulnerability assessments must be performed:

- Just prior to moving any website or web application into production. (Websites developed using CSUN's Web-One templates and published in CSUN's Web-One infrastructure do not require vulnerability assessments).
- Monthly for all websites and web applications, or at a timeframe deemed appropriate by the ISO based upon the risk.
- Just prior to moving major upgrades or changes to any website or web application into production.

Vulnerability Scanning Process

1. Campus website and web application owners must notify the Information Security Office (using the IT Help Center ticketing system or via email to iso@csun.edu) of all new websites (other than Web-One websites) and all new web applications before they are migrated into production.
2. Campus website and web application owners must notify the Information Security Office of all major upgrades or changes to their website or web application before the changes are put into production.

3. The Information Security Office will conduct vulnerability scans for websites and web applications and share findings with website and web application owners for review and, if necessary, remediation. The Information Security Office will work with the website and web application owners to schedule the most appropriate time to conduct the vulnerability scans.
4. Web applications must be scanned using authentication; therefore, the application owner must provide User ID credentials to the Information Security Office. The Information Security Office will submit a request for the account, specifying the level of access needed to scan the web application.
5. Vulnerability scan reports will be placed in a secure myCSUNbox folder unique to each website or web application owner and an email notification sent to the website or web application owner.
6. When CSUN is notified of an off-cycle critical patch released by a vendor to mitigate a vulnerability, the ISO will notify all affected website and web application owners of the necessity to implement the patch or remove the website or application from the network until the relevant patch is applied.
7. Vendor maintained web sites and web applications are subject to the same policies and standards as CSUN hosted websites or web applications. Vendors should provide to the owning department an audited attestation that they follow a vulnerability management and patching process, such as SSAE16 or PCI certification.

Remediation Process

At the completion of each vulnerability scan, campus website and campus web application owners must review the vulnerability report and ensure that vulnerabilities are remediated.

Discovered vulnerabilities must be remediated based on the following timeframes:

- Severity 3 and severity 2 vulnerabilities - within 30 calendar days of discovery.
- Severity 1 vulnerabilities - within 90 calendar days of discovery.

If a website or web application is found to be non-compliant and the problem is not resolved in the above referenced timeframe, the website or web application may be removed from the campus network. Exceptions must be approved by the Information Security Officer.