Vulnerability Scan Remediation

Purpose

This document provides a comprehensive scan and remediation procedure designed to help protect the systems managed at the CSU Fullerton.

Information Security Office (ISO) staff will identify potential threats and vulnerabilities through internal and external scans periodically. Thereafter, application teams (Responsible parties?) will be provided the scan results for remediation. The work to maintain a secure infrastructure environment is a collaborative effort between ISO, IT application teams, and Infrastructure Services staff by supervision of the management.

Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of CSU Fullerton services available both internally and externally as well as satisfy compliance with any relevant policies in place.

1.0 Scope

The scope of this procedure includes:

- The type and schedule of scans to be run
- Review and remediation of findings from scan reports
- Responsibilities of positions that will perform tasks

2.0 Definitions

Acceptable risk – Vulnerabilities identified in the scan but compensating controls are in place to mitigate the risk, or the service has been deemed critical and risk is accepted and approved.

Acceptable risk exceptions – Vulnerabilities that are recognized and it is determined that the risk is so low that it accepted and no further action is needed; or the financial cost of remediation is so great that it is not feasible to make changes to alleviate the vulnerability.

Data Owner – Management staff who approve access and changes to information/data of an application.

Data Steward – The individuals who make up the application teams and have the best ability to verify vulnerabilities and make recommendations for remediation.

False-positive – Vulnerabilities identified in the scan that are not vulnerabilities and do not cause a threat to the CSUF systems.

Acunetix Web Application Scanner (WAS) – Information Technology/Information Security Office provides the Acunetix Web Application Scanner (WAS) to allow application developers the ability to scan web applications in a

fully operational environment and check for many known security vulnerabilities. Acunetix checks web applications for common security problems such as SQL injection, cross-site scripting, command injection, buffer overflow, session management, and other vulnerabilities. Acunetix WAS is the approved tool to use on each web application release prior to deployment to a production environment, and on on-going bases after any new revisions or upgrades are introduced.

3.0 Responsibilities

Information Security Team – The basic role of the security team is to configure the scanning tool, run scans, prepare, review, and disseminate reports, and provide assistance.

Application Management – Management staff who are responsible for assigning individuals to review the scan report approve remediation and provide documentation to determine acceptable risk.

Application Teams/Infrastructure Services – Staff will review potential vulnerabilities and implement remediation recommendations. As appropriate, staff may take steps to reclassify, provide documentation and business justification to demonstrate vulnerability as false-positive or an acceptable risk.

Infrastructure Services – In addition to remediation responsibilities, Infrastructure Services staff will complete monthly patching according to the established schedule.

4.0 Procedures

Step 0 – Request Access to the Acunetix Web Application Scanner (WAS)

If you plan on using the WAS in your remediation efforts, you must first request access from the Information Security Team. Please email DG-IT-InfoSec@fullerton.edu to request an account and schedule training on how to scan your web applications for any vulnerabilities. The scan reports will includes detailed steps to remediate any vulnerabilities.

Step 1 - Run Scans and Prioritize Findings

ISO staff will run scans, according to the scan schedule and create reports. The reports list vulnerabilities as critical, severe, and moderate. Vulnerabilities should be addressed as a priority with focus on Critical and severe, moderate vulnerabilities as time is available. PCI requirements calls for remediating Critical and Severe vulnerabilities in 30 days. Ideally, all vulnerabilities should be addressed; however, ISO staff will work with application teams on the most significant first.

A web application is considered to be non-compliant if one of the following cases is true:

1. A critical (High or medium) vulnerability is not addressed or has not been remediated in a timely manner
2. A web application is not being scanned in accordance with the frequency defined

Below is the scan schedule:

Application Team	IP addresses	Scan time	Number of hosts

Step 2 – Review and Distribution of Reports

After reports are produced, ISO staff will provide a first level review of scans for critical vulnerabilities that affect servers with Level 1 data. Thereafter, the ISO will meet with application teams to discuss the results and provide assistance or an explanation of the findings.

ISO staff will also distribute the link to scan reports via email to application teams and Infrastructure Services staff.

Step 3 - Apply Patches

Patches are applied monthly as follows:

- Infrastructure Services staff will identify needed patches and submit a change request (CR) for approval.
- Infrastructure Services staff will install patches in the development and test environments on the Thursday following the release of Microsoft patches.
- Patches to the production environment will be installed on the following Sunday at 12:00 a.m.

5.0 Unresolved Issues and Vulnerabilities

If a vulnerability cannot be resolved through the normal patching process, ISO staff will suggest an alternative to alleviate the finding.

NOTE: The vulnerability continues to be recognized on reports until it is resolved.

On occasion, the data owner and ISO may determine a vulnerability cannot be resolved and the CSUF must recognize the exception as an acceptable risk. The data steward completes a *Security Risk Business Justification* form and submits it to ISO for approval.

In each of these cases, the CIO will be advised of the vulnerability and must approve the resolution.

6.0 References and Information

Appendix A – Security Risk Business Justification form (in Dropbox)

Appendix B – Visio diagram of workflow (in Dropbox)