CSUEB Business Process Guide

CSUEB Vulnerability Management

VERSION: 3.0
January 20th, 2017

Revision History

Version	Date	Action	Section	Updated By	Approved By
1.0	11/28/2016	Initial Document	All	Thomas Dixon	ISO
2.0	12/14/2016	Add Exception Request Section	Sections 4 & 5	Thomas Dixon	ISO
3.0	1/20/2017	Add Appendix A, Vulnerability Severity Levels Defined	Appendix A	Thomas Dixon	ISO

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE

A recent Information Security audit identified the need for the campus to implement vulnerability scanning, identification and remediation processes.

This business process guide provides the campus procedures for vulnerability management, including scanning, assessment, and remediation of the discovered vulnerabilities for CSU East Bay websites, applications and hosts. The results of scans are used to alert administrators to vulnerabilities, so that they can be remediated.

A vulnerability is a weakness which allows an attacker to reduce a system's information assurance and/or integrity. Such weaknesses can be a security exposure in an operating system or other system software or software component. Vulnerability scanners can locate these weaknesses and often provide information on the cause.

Relevant Standards

- ICSUAM §8045.00, Section "500 Information Asset Monitoring - …At a minimum, server administrators are required to scan regularly, remediate, and report un-remediated vulnerabilities on critical systems or systems that s tore protected information within a prescribed timeframe".

- ICSUAM §8070.S000, Section "1.6.2 Web and Application Testing and Change Management - Web applications should be scanned with an approved web application scanner prior to production deployment and periodically at a frequency determined by risk."

1.2 FREQUENCY

These processes will be performed both on a as needed and/or a scheduled basis.

As needed is defined as whenever a new web site, application or host image is ready to be release from an initial development or update stage.

Scheduled is defined as required regular periodic scanning of systems deemed to be of high enough risk by the system owner or Information Security Office.

Continuous is defined as the use of end-point management technology to scan and remediate vulnerabilities in university workstations, desktops, laptop. This process will not be covered in this guide – the "ITS Managed Software" guide covers this.

1.3 RESPONSIBLE PERSONS

These standards apply to all personnel who develop and deploy web sites, applications and host images at CSU East Bay. The target audience is anyone who has responsibility for designing, developing, reviewing and approving those same systems.

Vulnerability scanning, review and mitigation recommendations will be performed by the ISO Office.

2 VULNERABILITY SCANNING

2.1 VULNERABILITY SCANNING ROLES AND REQUIREMENTS

2.1.1. Roles and Responsibilities

2.1.1.1. Any campus personnel who have responsibilities to design, develop, review and/or approve new or updated web sites, applications, or hosts.

University web site, application and host administrators must notify the Information Security Office, via the ITS service desk of all new or upgraded web sites (other than Cascade websites), applications and host images before they are migrated into production.

2.1.1.2. The university Information Security office will conduct vulnerability scans, reviews and mitigation recommendations.

Vulnerability scanning is provided as a service by the Information Security Office. Questions about vulnerability scans and the need to schedule them should be directed to personnel in the Information Security Office via the campus service desk.

CSU East Bay's Information Security Officer is responsible for acquiring and managing an enterprise scanning and assessment tool for use on campus. If there is a desire or need to utilize a different vulnerability scanner, a request must be submitted to the ISO via the campus service desk.

It is important that the activity of vulnerability scanning is performed in consistent manner, utilizing the appropriate tool(s) for the systems to be scanned. The ISO can provide insight and assistance in determining and implanting the appropriate scanning tool(s).

2.1.1.3. External vendors (e.g. Cloud, PAAS, SAAS) who manage web sites, applications and hosts for the university are responsible to adhere to the same policies and standards as those maintained by CSU East Bay internally. Acceptable validation that a vendor performs the same levels of vulnerability management is an attestation which has been validated by an appropriate 3rd party auditor.

Vendors should present validation documentation during the initial acquisition process as well as at the outset of any renewal period. Acquisition or renewal of a product should not complete until a written risk statement is obtained from the ISO office.

2.1.2. Events Triggering Vulnerability Scanning Requirement

2.1.2.1. Any new or updated web site, application or host image cannot enter production without a vulnerability scan; this includes a review and mitigation of any discovered vulnerabilities.

2.1.2.2. Any web site, application or host deemed to be of high enough risk by the system owner or Information Security Office will undergo a regular periodic scan. Any discovered vulnerabilities found in the review of such scans must be mitigated on a schedule that reflects the risk of the vulnerabilities.

2.1.2.3. When the ISO office is made aware of a critical security patch through campus personnel, vendor or a 3rd party security organization.

2.1.3. Vulnerability Scanning and Review Procedures

2.1.3.1. The process to scan and review vulnerabilities consists of the following steps:

1. Requestor submits a request to scan a resource via the campus service desk.
    a. The submitter must provide logon credentials if the resource requires a login. However, the ISO office will need to complete an access request to obtain the account.

2. The ISO Office will schedule scan for the period(s) requested.

3. The scan completes and the ISO Office examines the results.

4. The ISO Office will work with requestor to interpret the results and discuss remediation(s).

5. Requestor will implement remediation(s) and notify the ISO Office contact when completed.

6. ISO Office will re-run scan, if issues remain, ISO Office will repeat the process until the requestor has remediated found vulnerabilities (or an exception is requested and granted).

7. If this is a scheduled periodic scan, the process repeats from step 3 each time the scan reoccurs during the schedule; otherwise the scan and remediation processes are considered to be completed.

8. The results of the scan, the application of remediation steps and results of the re-scan of the resource will be kept in the campus service desk records.

3 VULNERABILITY REMEDIATION

3.1 VULNERABILITY REMEDIATION ROLES AND REQUIREMENTS

3.1.1. Roles and Responsibilities

3.1.1.1. When a vulnerability scan completes, the ISO office must review the scan and recommended mitigations.

3.1.1.2. At the completion of each vulnerability scan the requestor must review the vulnerability report and proposed mitigations from the ISO office. The requestor must then implement the appropriate mitigations and notify the ISO office that the mitigations have been applied, and to request a re-scan.

3.1.2. Timeframes for Remediation of Vulnerabilities

3.1.2.1. Discovered vulnerabilities must be remediated based on the following timeframes:

Urgent and Critical (Levels 5 & 4) * vulnerabilities must be completely remediated as soon as possible, but no longer than 30 calendar days of being reported.

Serious, Medium and Low (Levels 3, 2, & 1) * vulnerabilities should be remediated at the next regular maintenance cycle, but no longer than 90 calendar days of being reported.

3.1.2.2. If a vulnerability is not remediated within the above referenced time frames (according to severity) the service or device may be taken offline. Exceptions have to be requested and approved by the Information Security Officer, or CIO, if the ISO is not available. Please see section “4 – Exception Requests” to understand how exceptions are requested and approved.

3.1.3. Definition of a Remediated Vulnerability

3.1.3.1. A vulnerability is considered to be remediated when a post mitigation scan shows that the vulnerability no longer exists. Most vulnerabilities are remediated by applying updates, upgrades and/or patches; occasionally resolution comes through a change to configuration. Lastly, the method of remediation should be recorded in the service desk ticket the request originated from.

*For definitions of the severity levels, please see “Appendix A – Vulnerability Severity Levels Defined”.

4 EXCEPTION REQUESTS

4.1 EXCEPTION REQUEST ROLES AND REQUIREMENTS

Relevant Standard: 8020.S000 Information Security Risk Management – Exception Standard

There are many reasons that a vulnerability cannot be remediated. A system may no longer be supported by a vendor because it is end of life or the vendor is no longer in business, a patch may be late from the vendor, some vulnerabilities exist during the normal operation of a service (or at least the scan tool identifies a normal operation as a vulnerability). Whatever the case, an exception to mitigating an identified vulnerability may be required.

Exceptions to standard vulnerability remediation must be requested through the ISO office. The request must come from appropriate administrator (manager) responsible for the system. The approval of an exception may involve additional persons outside of the ISO office. Such as the appropriate data steward, system owner, CIO, AVP, etc.

Approved exceptions are not permanent and are subject to periodic review by the Information Security Office so that the exception is not kept in place indefinitely.

4.1.1. Roles and Responsibilities

4.1.1.1. The requestor of a vulnerability exception must provide the following information in writing to the ISO office via the campus service desk:

a. The general reason and/or justification for the exception (patch will break application, vendor no longer supporting product, etc.)
b. The long-term plan to remediate the vulnerability or retire the affected system.
c. Any proposed compensating controls to mitigate the risk.
d. The name of the campus administrator that will accept the risk.

4.1.1.2. The campus ISO office will:

a. Review the exception request to verify the justifications, proposed remediation and compensating controls.
b. Identity and propose any alternative mitigations (from an information security posture only).
c. Perform a risk evaluation and present it to the campus administrator accepting the risk as identified in the exception request.
d. If the exception is granted, the ISO office will record the exception in the campus service desk application.
e. Periodically review the exception until it is no longer required.

5 RETENTION OF RECORDS

- The CSUEB Information Security Office requires administrators of campus system to create service tickets to request onetime and/or regular scanning of systems for vulnerabilities.
- Such tickets will contain the relevant information on scan results and mitigation recommendations and serve as a record of those scans and remediation of findings.
- 5 years of data will be retained.

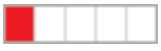
APPENDIX A – VULNERABILITY SEVERITY LEVELS DEFINED

Vulnerability Severity Level Definitions
When a vulnerability scan completes, any found vulnerability will be given a severity level. The higher the severity, the greater the need to mitigate the vulnerability as soon as possible.

For purposes of applying mitigations to found vulnerabilities, the ISO office will expect that those with severity levels "Urgent and Critical" will be resolved as soon as possible. This includes the possibility of interrupting availability of a service in order to implement a mitigation to resolve the vulnerability.

Vulnerabilities with severity levels of "Serious, Medium, and Low" are more likely to have acceptable work arounds and/or mitigated by other factors not shown in the results of the scan. For vulnerabilities with these severity levels, if mitigation is required, it can be done during regular maintenance cycles instead of as soon as possible.

Exceptions – See section "4 – Exception Requests" to understand how an exception can be requested and approved.

SEVERITY	**LEVEL**	DESCRIPTION
	**Urgent**	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.
	**Critical**	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	**Serious**	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	**Medium**	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	**Low**	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.