CITY UNIVERSITY OF HONG KONG
Vulnerability Management Standard

(Approved by the Information Strategy and Governance Committee in Jan 2024)

INTERNAL **Date of Issue: 2024-01-11**

Document Control

Document Owner	Classification	Publication Date
CSC	INTERNAL	2024-01-11

Revision History

Version	Date	Summary of Changes
1.0	2024-01-11	Initial Release

Distribution

Copy	Issued to	Location
Master	Internal	https://www.cityu.edu.hk/csc/information-security/information-security-policies-and-standards

Contents

1 Policy Statement

In compliance with the University Information Security Policy, the University will conduct vulnerability scans to detect potential internal and external threats to University Data. The objective of this Standard is to establish standard requirements for the University's process of identifying, evaluating, and resolving vulnerabilities.

2 Objective

The purpose of this document is to establish a security standard for managing technical vulnerability found in campus network environment. This standard is based on National Institute of Standards and Technology (NIST) 800-53, specifically the Risk Assessment (RA-5) Vulnerability Scanning section. It provides a framework for performing vulnerability scans and corrective actions to protect the Campus Network.

3 Scope

This Standard applies to University Technology Resources connected to the Campus Network. It does not apply to content found in email or digital documents.

4 Terms and Definitions

4.1. “Authenticated Scan” means a vulnerability scan performed as a logged-in authenticated user.

4.2. “Authentication” means verifying the identity of a user, process, or device to allow access to a University Information System.

4.3. “False Positives” means incorrectly classification of a benign activity as malicious or vulnerability.

4.4. “Mission Critical Services” means a service required to conduct the essential mission-oriented operations of the University, including teaching and learning. Unplanned interruptions in service have an immediate and widespread impact on critical University operations and typically result in a very negative customer experience. Examples include AIMS, Banner.

4.5. “Risk” means the relative impact that an exploited vulnerability would have to a user’s environment.

4.6. “Threat Likelihood” means the likelihood or frequency of a harmful event occurring.

4.7. “Senior Management” means vice presidents, assistant vice presidents, associate vice president, deans, or directors of the University.

4.8. “Unauthenticated Scan” means a vulnerability scan performed to identify vulnerabilities that are accessible without logging in as an authorized user.

4.9. “Vulnerability Scan” means a technique used to identify weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or trigger by a threat source.

4.10. “Vulnerability” means a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability.

4.11. “Agent Scan” means a lightweight, low-footprint programs installed locally on hosts. The agent can report detailed information to centralized platform without providing credential information.

5 Responsibilities

5.1. The Chief Information Officer, supported by Information Security Unit, is responsible for the implementation and enforcement of this Standard.

5.2. Information Security Unit (“ISU”) is responsible for administering the network Vulnerability scanning tool (“NetScan”), Agent Scan tool and the web application scanning tool (“AppScan”) and for keeping both updated with the information and signatures of the latest Vulnerabilities that can be exploited as well as conducting Vulnerability scans pursuant to the requirements identified within this document.

5.3. All System Owners are responsible for providing the documentation required to facilitate a Vulnerability scan and remediating vulnerabilities detected within the University Information System(s) they oversee.

5.4. Head of Department, assisting by their departmental network administrator (DNA), are responsible for ensuring the University Technology Resources they oversee are scanned, remediating vulnerabilities identified, and identifying all False Positives.

5.5. System administrators are responsible for ensuring the devices they manage and keeping the operating systems and software kept up to date.

6 Vulnerability Classification

All Vulnerabilities detected by ISU scanning tools are assigned a severity level based on the National Vulnerability Database Common Vulnerability Scoring System (“CVSS”) Base Score Metrics: Critical, High, Medium, Low, or Informational.

- **Critical**. Indicates flaws could be easily exploited by an unauthenticated remote attacker and lead to compromise (CVSS Score 9.0-10.0).
- **High**. Indicates local users can gain privileges, allow unauthenticated, remote users to view resources that should otherwise be protected by authentication, allow authenticated remote

users to execute arbitrary code, or allow remote users to cause a denial of service (CVSS Score 7.0-8.9).

- **Medium**. Indicates flaws may be more difficult to exploit but could still lead to compromise under certain circumstances (CVSS score 4.0-6.9).
- **Low**. Indicates Vulnerabilities require unlikely circumstances to be able to be exploited or where a successful exploit would cause either no adverse effect or result in minimal adverse consequences (CVSS score 0.1-3.9).
- **Informational**. Useful information that is more general information about the system and how it operates. Mostly configuration choices rather than a real vulnerability (CVSS score 0).

7 Campus Network Scans

7.1. The following Vulnerability scans (workflow refer to Appendix A) are conducted to detect security weaknesses within the Campus Network:

(a) Bi-weekly Unauthenticated Scans of individual IP addresses of University Technology Resources deployed on the Campus Network;

(b) Authenticated Scans or Agent Scans of IP addresses as requested;

(c) Monthly Scan of all public IPs owned by University from outside of the Campus Network ("External").

7.2. Attempts to block scans or access from the network Vulnerability scanner are prohibited.

7.3. Use of tools that are used to assess security or to attack computer systems or networks (e.g., password crackers, vulnerability scanners, network sniffers) without Central IT authorization is prohibited.

7.4. Vulnerabilities identified in campus network scans must be follow-up and remediated as follows:

(a) Critical / High must be remediated or mitigated immediately.

(b) Medium must be remediated or mitigated within 90 days of discovery.

(c) Low must be remediated or mitigated within 180 days of discovery.

8 Web Application Scans

8.1. Authenticated Scans are required for those University Information Systems stored or processed CONFIDENTIAL / RESTRICTED information.

8.2. Information System Owners must complete the Web Application Scans Form (refer to Appendix C) to facilitate a web application scan.

8.3. Web application scan shall be performed (a) new Internet-facing web applications, (b) web application with major change. Workflow refer to Appendix B.

8.4. Vulnerabilities discovered in Web Application Scan must be follow-up and remediated as follows:

1. Critical / High must be remediated or mitigated immediately.
2. Medium must be remediated or mitigated within 90 days of discovery.
3. Low must be remediated or mitigated within 180 days of discovery.

8.5. Critical / High Vulnerabilities directly related to missing security patches must be evaluated within 60 days of the patch being released.

8.6. Remediation scans will be conducted to validate remediation of identified High/Critical Vulnerabilities.

8.7. If a Vulnerability cannot be remediated, compensating controls must be put in place to mitigate the Vulnerability.

8.8. University Technology Resources with Critical/High Vulnerabilities that are not remediated will be blocked from connecting to the Campus Network.

9 Critical Patching

9.1. All available security patches for critical vulnerability ("critical patches") must be follow-up immediately.

9.2. Following the change management standard, critical patches must be tested on testing environment before being rolled out to production.

9.3. Some critical patches may require reboot that end users shall reboot their devices in order to apply the updates properly.

9.4. Critical Patches that cannot be implemented within 30 days must be submitted as a compliance exception indicating the compensating controls that will be implemented. This includes instances when a vendor does not provide a Critical Patch to remediate a Critical and Exploited Vulnerability.

9.5. Critical Patches released by a vendor outside of their normal release cycle released to address a previously unknown exploit ("zero-day exploit") must be installed immediately.

9.6. In the instance that a Critical Patch addresses a Critical Vulnerability that poses a significant risk to the University, Information Security Unit will notify Departmental Network Administrators to expedite installation.

10 Exceptions

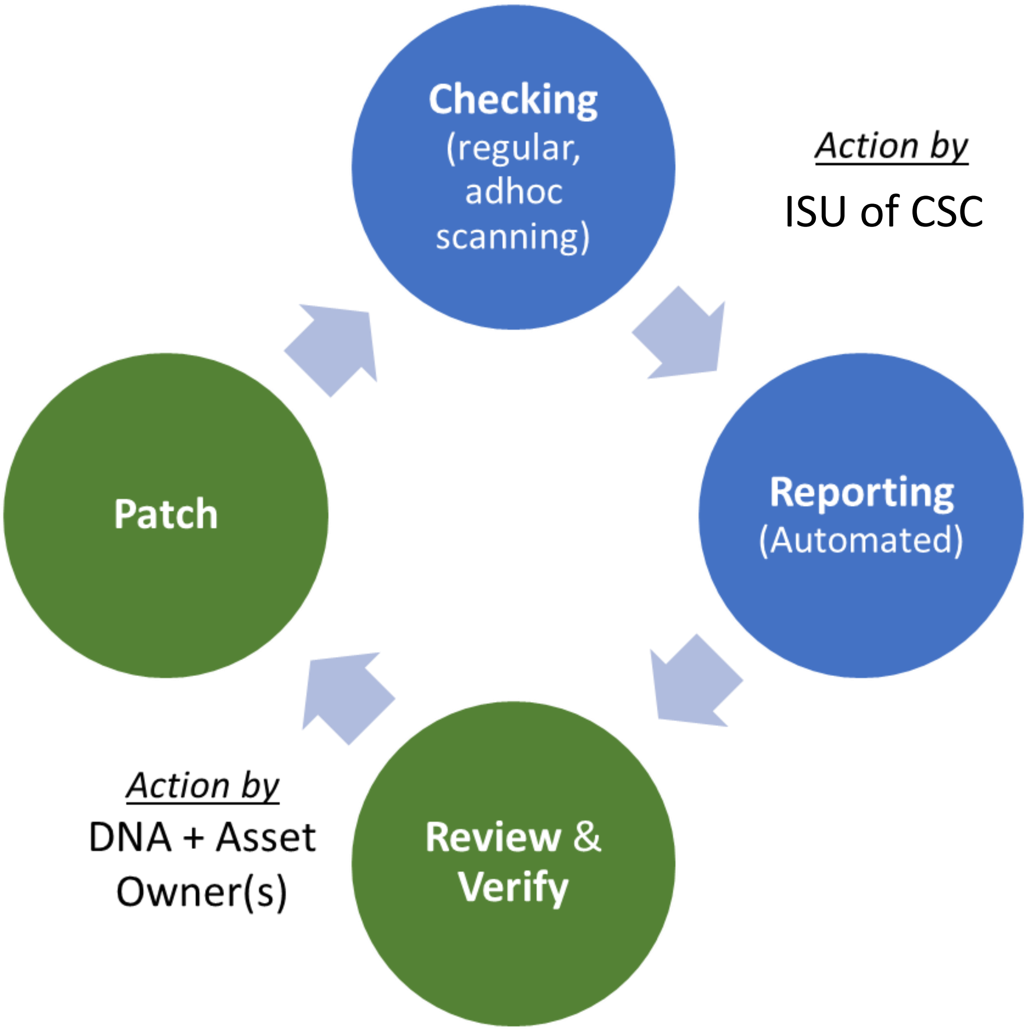
10.1. Application not under direct control of the University and function outside of the Campus Network will not be scanned.

Reference

The following documents were consulted during the preparation of this document:

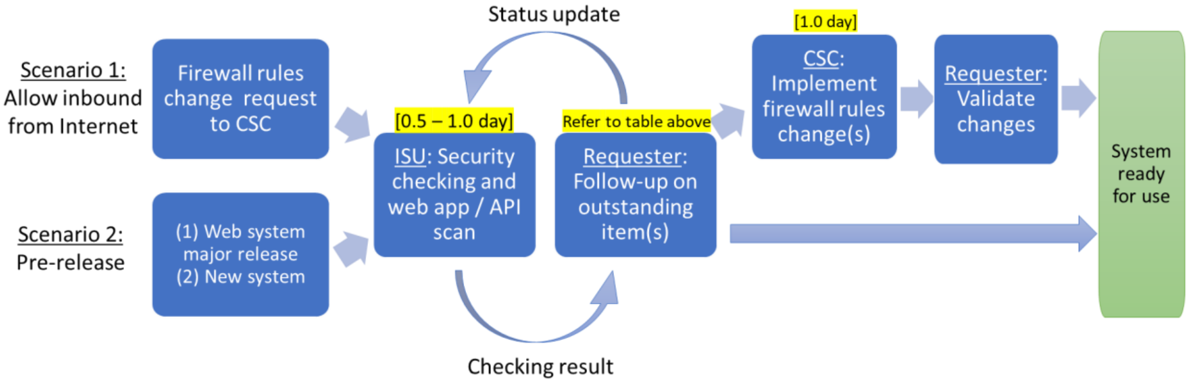
- City University of Hong Kong, Information Security Policies and Standards (ISPS)
- City University of Hong Kong, Acceptable Usage Standard
- NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations

Appendix A – Campus Network Scans Workflow



Appendix B – Web Application Scans Workflow

Severity	Target Time to fix
Critical	Immediate
High	Immediate
Medium	90 days
Low	180 days


Status update
Scenario 1:
Allow inbound from Internet
Firewall rules change request to CSC
[0.5 – 1.0 day]
ISU: Security checking and web app / API scan
Refer to table above
Requester: Follow-up on outstanding item(s)
[1.0 day]
CSC: Implement firewall rules change(s)
Requester: Validate changes
System ready for use
Scenario 2:
Pre-release
(1) Web system major release
(2) New system
Checking result

Appendix C – Web Application Scans Form

Please complete the following information to initiate a Web Application Scan:

- Requester's Name: ___________________________
- Requester's Department: _______________________
- Application Name/URL: _________________________
- Application Description: _______________________
- Application Owner/Contact Person: _______________
- Scan Start Date (if specific date is required): ______________
- Scan Completion Deadline (if applicable): ____________
- Additional Information or Requirements: _________________________
- Login account (if any):_____________
- Highest data classification of the system:
  RESTRICTED / CONFIDENTIAL / INTERNAL / PUBLIC

Note: Please provide any supporting documentation, such as network diagrams or system architecture diagrams, if available and relevant to the scan.

By signing this form, you acknowledge that you have read and understood the Vulnerability Management Standard and agree to comply with University Information Security policies and Standards.

Requester's Signature: ___________________________

Date: ___________________________