Vulnerability Management Procedure

Background

In support of the Vulnerability Management Policy, university owned or operated information technology systems, computing and non-computing (IoT), and devices accessing the university network are regularly scanned by the Office of Information Security (OIS) for vulnerabilities. Systems with open vulnerabilities present varying levels of risk to data and other systems depending on the severity of said vulnerabilities. The purpose of this procedure is to provide an outline for the management process of identified vulnerabilities on UC's network.

Procedure

Scanning

- Agent Based - The installation of vulnerability scanning agents should be leveraged for all university owned assets whenever possible to allow for regular, internal vulnerability scans. Agent-based scans provide the most accurate and up-to-date information.
- Automated - Scheduled scans of all technology assets on UC's internal and external networks are conducted monthly. Due to the size of the environment, some scans may take a significant amount of time, but all scans will be completed within 30 days of initiation. Scanning frequency may be adjusted in the event of a compromise, actual or anticipated release of a major vulnerability, or another event that carries significant risk to the university. Network scans from the university's vulnerability scanning solution must be permitted to scan private networks, VLANS, and behind firewalls, load balancers, and other networking equipment unless pre-approved and documented by OIS.
- Manual - Manual scans of systems or network segments can be conducted on demand and initiated either by OIS or by technical personnel as defined below.
- External - An annual external scan will be conducted by an independent third-party engaged by OIS. The scan will focus on critical systems and assets as determined by OIS.

Roles and Responsibilities

Technical Personnel may include Data Custodians, Data Stewards, System Owners and Administrators, or other university community members responsible for the operation and management of systems and servers which store or provide access to institutional data. These users are required to complete Qualys user training prior to gaining access to the enterprise vulnerability scanning platform.

Each department must identify at least one user to serve in the capacity of primary or first level contact, typically an IT administrator or user with operational responsibility for IT assets.

Additional users, typically supervisors or managers within the department, may be identified as secondary or second level contacts. These users are responsible for addressing unremedied vulnerabilities prior to escalation to Department Heads.

If a point of contact needs to be updated, this should be communicated to OIS.

Vulnerability Rating

To aid in prioritization of remediation, a rating is assigned to each identified vulnerability based on industry standard practices and university risk tolerance.
OIS will facilitate rating of vulnerabilities through an approved enterprise vulnerability management platform. Please review the following rating definitions and remediation requirements.

Bearcat Risk Index (BRI)

Bearcat Risk Index is a university internal scoring system managed by OIS to assist departments and Technical Personnel in prioritizing remediation of vulnerabilities that present the most acute risk to the university systems or data. The BRI is based on industry standard vulnerability criticality ratings, university asset priority, and current threat profile. The numeric level rating used in the calculation is assigned by the enterprise vulnerability scanning platform.

- **BRI – Out-of-band**
  Out-of-band significant vulnerabilities as deemed by OIS or university leadership must be remediated as soon as possible, but no later than 7 days. Due to the extremely critical nature of these vulnerabilities, exemptions are not available without executive leadership approval and documentation.
- **BRI - Critical (Level 5)**
  Critical level vulnerabilities must be remediated as soon as reasonably possible, but no later than 30 days after release.

- **BRI - High (Level 4)**
  High level vulnerabilities must be remediated as soon as reasonably possible, but no later than 45 days after release.
- **BRI - Moderate (Level 3)**
  Moderate level vulnerabilities must be remediated as soon as reasonably possible, but no later than 60 days after release.
- **BRI - Low (Level 2)**
  Low level vulnerabilities must be remediated as soon as reasonably possible, but no later than 90 days after release.
- **BRI - Informational (Level 1)**
  Informational vulnerabilities are often deviations from industry best practice and when possible, should be remediated within 180 days.

BRI – High Risk Assets

BRI - High Risk Assets, also tagged as "Qualys TruRisk" on the departmental vulnerability dashboard, present the most significant risk to UC and will have the greatest risk reduction effect through remediation.

Vulnerability Reporting

To support timely remediation of vulnerabilities by responsible Technical Personnel, OIS will focus reporting only on assets confirmed as university owned.

Reporting will be conducted via department specific dashboards within the enterprise vulnerability scanning platform that identify vulnerability ratings. These dynamic dashboards will update on a regular basis, multiple times per day in most cases. Technical Personnel must review dashboards and perform vulnerability remediation. If an asset listed is not in their area of responsibility or if remediation of a vulnerability cannot be automatically identified by the enterprise vulnerability scanning platform, Technical Personnel should contact OIS.

To ensure proper communication of confirmed vulnerabilities to departments, the following escalation process will be followed:

Notification

- Department identified primary and secondary contacts will have real-time access to vulnerability data through a dynamic dashboard within the enterprise vulnerability scanning platform.

Department Head Notification

- A quarterly summary report will be provided to the VP, Dean, or Department head of all currently open vulnerabilities for the unit.

Disconnect

- System may be removed from the network, or its services limited if an open BRI-Critical or BRI-High (level 4 and 5) vulnerability is not remediated in 120 days.

Out-of-band Escalation

- BRI - Out-of-band vulnerabilities may be escalated to department and university leadership as deemed necessary or if not remediated within 14 days.

Remediation

When an open vulnerability is no longer identified on an automated scan or via an installed agent, OIS will consider it remediated. If the same vulnerability is identified in the future, it will be treated as a new vulnerability.

Definitions

Technical personnel - Data Custodians, Data Stewards, System Owners and Administrators, or other university community members responsible for the operation and management of systems and servers which store or provide access to institutional data.

Out-of-band catastrophic vulnerability patch - An emergency software or operating system patch that is deployed immediately and prior to the next routine restart, usually driven by known significant impact to systems or data, or active exploitation, example zero-day vulnerability exploit.

Zero-day vulnerability - A vulnerability in a system or device that has been disclosed but is not yet patched. An exploit that attacks a zero-day vulnerability is called a zero-day exploit.

Contact Information

Office of Information Security	513-558-ISEC(4732)	infosec@uc.edu

Related Links

Vulnerability Management Policy

History

Revised: 6/01/2023