University of CINCINNATI

Vulnerability Escalation Procedure

Background

In support of the Vulnerable Electronic Systems Policy, electronic systems on the University of Cincinnati (UC) network are regularly scanned by the IT@UC Office of Information Security (OIS) for vulnerabilities. Systems with open vulnerabilities present varying risks to data and other systems on the UC network depending on the severity of said vulnerabilities. The purpose of this procedure is to provide an outline for the escalation process of discovered vulnerabilities on UC's network.

Procedure

Scanning

- Internal Automated - Scheduled scans of all technology assets on UC's internal network are conducted on monthly basis. 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.
- Manual - Manual scans of systems or network segments can be conducted on demand and initiated either by OIS or by Data Custodians as defined below.
- External - An annual external scan will be conducted by an independent third party entity engaged by OIS. The scan will focus on critical vulnerabilities and assets as determined by OIS and/or consultant.

Vulnerability Scoring

To aid in prioritization of remediation, a score is assigned to each identified vulnerability based on industry standard practices. The IT@UC Office of Information Security has determined that Qualys will serve as the university's enterprise vulnerability scanning solution, producing a Level 1-5 scale listed in the definition section. The IT@UC Office of Information Security deems Level

5 and Level 4 vulnerabilities as catastrophic, requiring immediate attention and remediation.

Escalations

To facilitate remediation of vulnerabilities with the highest risk to the university data, OIS will focus escalation solely on business production systems with static Internet Protocol (IP) addresses. The IT@UC Office of Information Security does not generally escalate vulnerabilities on dynamically addressed systems, but may choose to do so in the event of a major vulnerability, compromise, or investigation.

Escalations will be conducted via an enterprise ticketing system or via email, as applicable. Data Custodians are responsible for reviewing escalations and notifying OIS if assets listed are not in their area of responsibility, or if action has been taken to remediate them.

To ensure proper communication of identified vulnerabilities to Data Custodians responsible for remediation, the following escalation process will be followed:

Notification

- Data Custodian is notified of a newly identified catastrophic vulnerability via an enterprise system (ticket management or email).
- Follow-up notification will be provided after 30 and 60 days following an automated rescan.

Escalation to Level 2

- Data Custodian and their supervisor are notified of an open catastrophic vulnerability that has not been remediated after initial notification for 90 days.

Escalation to Level 3

- Data Custodian and their supervisor are notified of an open catastrophic vulnerability that has not been remediated after initial notification for 120 days.
- Department manager may be notified at OIS discretion or system may be disconnected from the network.

Disconnect

- System may be removed from the network or its services limited if an open catastrophic vulnerability is not remediated in 180 days.

Remediation

When an open vulnerability is no longer identified on an automated scan, OIS will consider it remediated and close the issue. If the same vulnerability is identified in the future, it will be treated as new. Data Custodians may notify OIS of remediation and request verification by a manual scan.

Data Custodians are responsible for remediation and management of all vulnerabilities, regardless of assigned score, discovered during scanning.

Definitions

Data Custodian - computer system administrators responsible for the operation and management of systems and servers which store or provide access to institutional data.

Level 5 (Catastrophic) - Intruders can easily gain control of the system, 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.

Level 4 (Catastrophic) - Intruders can possibly gain control of the system, 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 system.

Level 3 (Critical) - Intruders may be able to gain access to specific information stored on the system, including security settings. This could result in potential misuse of the system by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the system, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.

Level 2 (Moderate) - Intruders may be able to collect sensitive information from the system, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

Level 1 (Low) - Intruders can collect information about the system (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

Vulnerability scoring scale – Numeric scale used for quantifying severity of a vulnerability as defined by Qualys.

Contact Information

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

Related Links

Vulnerable Electronic Systems Policy
Data Governance & Classification Policy

History

Issued: 11/21/2016
Revised: 1/28/2019