Vulnerability Management Standard

Issued Date: 16-February-2015
Effective Date: 01-July-2015

Purpose

This standard establishes a framework for identifying and remediating vulnerabilities that could impact the university's data, systems, or services.

Vulnerability management is the process of identifying vulnerabilities, classifying their potential impact, and determining a qualitative risk score in order to prioritize the remediation of vulnerabilities. Vulnerability management is a critical component of the university's information security program. Failure to comply with this standard could impact the confidentiality, integrity, and availability of university data, systems, and services. Following a risk-based approach, systems that transmit, store, or process restricted data should always be remediated before other systems.

Scope

This process applies to:

- All university-owned IT assets
- All systems that transmit, process, store or access university data or resources

Definitions

In the context of this document, the following terms are used as indicated here:

- **Vulnerability** – A vulnerability is a weakness in a product (operating system or software application) that could allow an attacker to compromise the integrity, availability, or confidentiality of that product or its data.
- **CVSS** – Common Vulnerability Scoring System is a scoring system designed to provide an open and standardized method of rating the potential impact and severity of IT vulnerabilities.
- **Critical** – Vulnerabilities with a CVSS score of 9.0 and higher, or that have been specially designated by the University Information Security Office (UISO) must be mitigated as soon as possible, but no later than five business days after notification.
- **High** – Vulnerabilities with a CVSS score between 7.5 and 8.9 must be patched no later than two weeks after notification.
- **Moderate and Low** - Vulnerabilities with a CVSS score of 7.4 or lower should be patched no later than one month after notification.
- **OU** - Organizational Unit. This is an administrative unit such as a Campus, College, School, Department, Office, or Team within the university. In some cases an OU may span across multiple reporting structures, for example, an IT project that involves individuals from multiple departments.
- **Compensating Control** - Additional settings or software installed to reduce the risk of the vulnerability while not applying the vendor's software patch.
- **System Administrator** – Any employee, affiliate, contractor, or vendor of the university who has administrative and/or operational responsibility over university data and/or technical systems. In some cases, an OU may have multiple system administrators.

(continued)

Roles and Responsibilities

University Information Security Office (UISO)

The UISO will perform the following:

- Scheduled vulnerability scans and management of results
- Notifying the OU security contact of critical or high results
- Track remediation progress and generate reports for the appropriate university officials
- Manage the removal process for noncompliant systems

Organizational Unit (OU)

In accordance to university policy IT 3.0 (IT 3.00, II.A.5) the management staff of each organizational unit is responsible for the security of its IT assets. Additionally, each OU must ensure the UISO has proper contact information for the networks and devices you are responsible for.

System Administrator

University policy IT 1.06 (IT 1.06, II.A.3) states that system administrators must maintain IT systems in accordance with the university's information security program[1]. Each administrator must monitor vendor websites and mailing lists for security patches for software they manage. These updates must be applied according to criticality. If no system administrator is defined, the responsibility goes to the organizational unit manager.

University Officials

Any one of the following University officials, CIO, Deputy CIO, CISO or data steward is authorized to approve exceptions to the network removal process.

Procedure

Notification Process

1. The UISO will perform regularly scheduled vulnerability scans of devices. When a vulnerability meets the Critical/High designation, a notification will be sent to the designated security contact for the OU.
2. The system administrator must verify the presence and/or applicability of the vulnerability on their system no later than two days after notification. Systems that can be accessed from the Internet should be remediated first.
    a. *If they believe this is a false positive, the questions in Appendix A must be submitted, as a service ticket, to the UTS Service desk.*
3. The system administrator must apply the mitigation or compensating control for the vulnerability.
4. Testing the system or service to ensure it is secure will primarily be the responsibility of the owning group.
5. Once the system owner feels remediation is complete, they should notify the UISO via the service desk ticket.
    a. *UISO may test independently to verify the results and will coordinate with system owner.*

Removal from the Network

If a system administrator does not remediate the vulnerability within the specified guidelines, as defined in the definitions section of this document, the system will be out of compliance. Non-compliant systems are subject to removal from the network. Removal will occur at the discretion of any of the following people: CIO, Deputy CIO, CISO or data steward. Additionally, the owner of the system or service can voluntarily remove the vulnerable system or service from the network.

When instances of systems or services must remain connected, due to business needs, to the network in a vulnerable state past the listed remediation window; and, the systems or services ***contain restricted data,*** *approval for an exception must be received from any of the following: CIO, Deputy CIO, CISO or data steward.*

(continued)

[1] http://sc.edu/about/offices_and_divisions/university_technology_services/security/security_program/

1. If a system or service is removed from the network by the UISO, the OU manager, data steward, CIO and Deputy CIO will be notified of this event.
    a. *The owning group should post an outage notification if appropriate. Responsibility for this communication falls on the owning group.*
2. Once both the OU and the CISO are satisfied with the results of the vulnerability assessment, the system or service can be put back into production.

Exception Process

Verification

If the vulnerability is deemed not applicable or cannot be confirmed by either the UISO or the OU, the system administrator will submit the Appendix A report within two business days of notification to the UISO and the OU manager.

Cannot meet deadline

If the system or service will not be secured within the specified time, the system administrator will submit the Appendix B report within two business days of notification to the UISO, the Deputy CIO and the OU manager.

Report a Vulnerability

When a system or service vulnerability is identified, it must be brought to the attention of the responsible group as well as the UISO via UTS service desk ticket.

Responsibility for Implementation

UTS management, data stewards, university officials and/or the owner of the system will be responsible for responding to risk associated with a given vulnerability.

Enforcement / Consequences

The UISO will coordinate verification of vulnerabilities with the OU. The UISO will escalate any deficiencies or problems to the CISO as well as the Deputy CIO or the data stewards. Systems or services will also be taken offline until this procedure is met. Other disciplinary action may be taken as appropriate.

Related Documents

http://www.sc.edu/policies/univ150.pdf
http://www.sc.edu/policies/it106.pdf
http://uts.sc.edu/itsecurity/program/datasecuritychecklist.shtml
http://www.first.org/cvss
http://www.sc.edu/policies/it300.pdf

Contacts

http://security.sc.edu

Revision History

Author	Date	Comments
Tom Webb		Published Version 1.0
Kyle Brown	8-Apr-2015	Formatting

(continued)

Appendix A (False Positive)

Has the vulnerability been confirmed?

Why do you believe the system is not vulnerable?

Which data classification is the information stored or processed by the vulnerable system or service considered (public, limited, or restricted)?

Who is the data steward of this data?

Appendix B (Unable to remediate)

Which data classification is the information stored or processed by the vulnerable system or service considered (public, limited, or restricted)?

Who is the data steward of this data?

Is this system accessible from the Internet?

What function does the vulnerable system or service provide?

Does the vulnerable system or service have additional protections to reduce the risk, if exploited?

Why can't the vulnerable system or service be secured in the specified time frame?

How long will it take to secure the vulnerable system or service and what resources will be required to do so?