Computer Services Center
Vulnerability Management Policy

Policy Issued: April 25, 2018

I. Summary

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities that may lead to security or business risk. The Computer Services Center (CSC) is dedicated to securing the network by enforcing proper vulnerability management practices. This policy includes roles and responsibilities of groups, personnel, the vulnerability management process and procedure, and the risk assessment and priorities of identified vulnerabilities.

II. Scope

This Policy establishes a framework for identifying and promptly remediating vulnerabilities to minimize security breaches associated with unpatched vulnerabilities and applies to all CSC servers and appliances both physical and virtual.

III. Roles and Responsibilities

The Assistant Vice President and Director Information Technology Services (AVPDITS) is responsible for the Computer Services Center's (CSC) vulnerability management. The key roles for vulnerability management are as follows:

Office of Information Security – Performs monthly vulnerability scanning to identify vulnerabilities, patch releases, and remediation plans.

Asset Inventory List – An inventory of Computer Services Center (CSC) assets.

Administrator (System or Application) - Generally, a University staff member who manages and maintains computer devices for the University and is authorized to have access beyond that of an end user.

Computer System and Software Specialist - Performs remediation of vulnerabilities (patching or compensating control) on servers, applications, operating system, or appliances based on the severity level and time for remediation (see Table 1).

Associate Director of Information Systems, Director of Academic Computing, and Assistant Director of Networking and Telecommunications – Determines scheduling of remediation of vulnerabilities, for their respective areas, and delegates corrective action. Report any unresolvable vulnerability to the Director of Information Security.

Director of Information Security (DIS) Role – Tabulates monthly vulnerability results and creates the monthly Vulnerability Report for distribution to directors/managers. Reports any unresolved vulnerabilities to the AVPDITS. Responsible for the vulnerability management program/policy.

Assistant Vice President and Director Information Technology Services (AVPDITS) Role – Approves any risk acceptance, emergency remediation actions and final report of monthly scans.

IV. Vulnerability Management Process and Procedure

The Computer Services Center goes through a continuous cycle of scanning and remediating vulnerabilities through a series of monthly network scans. The procedures associated with the vulnerability management process are as followed:

- *Scan CSC Servers, appliances, and VMs for vulnerabilities* – CSC Assets are scanned monthly. Each asset is scanned against a single baseline vulnerability policy based on the CVSS model (see paragraph IV).
- *Validate findings from scan and asses the risk severity* – The Office of Information Security will verify the scan results. This is done by negating false positives or taking additional steps to validate exposure.
    - Note: To greatly increase the accuracy of the scan and decrease the chance of "false positives", assets will be scanned via an authenticated or credentialed scan. This can be done with public key exchange or creating an account with administrator privileges (local administrator or Windows domain administrator) for the most accurate security assessment and recommended fixes for the system. This allows the scanning engine to collect information based on system configuration. Less than administrator privileges limits the scan to fewer checks and the results will not be as complete.
- *Inform the Director of Information Security* – Every month, the results of each vulnerability scan are made available to the DIS. The DIS will distribute the monthly Vulnerability Report to the Associate Director of Information Systems, the Director of Networking and Telecommunications, and the Director of Academic Computing.
- *Remediate Vulnerabilities (patching)* – ACAD, Information Systems, and Networking groups will develop procedures/processes to remediate each vulnerability class based on Table 1. Patching can be automated. If a vulnerability cannot be remediated, based on the Table 1 schedule, the director will provide a reason for the delay and a remediation plan to the DIS before the next month Vulnerability report. Critical vulnerabilities with immediate impact are expedited and resolved as soon as possible.
- *Non mission critical servers* – Non mission critical Windows servers must have auto updates enabled or the owner must email the DIS stating why auto updating cannot be enabled and that patches will be applied manually, every month, as described in Table 1.
- *Build and implement vulnerability resolution* – Once a patching process/plan is developed, the respective area proceeds with implementation.
- *Unsupported O/S* – CSC assets running unsupported operating systems must be upgraded, replaced before manufacturer support ends, or removed from the network.
- *Post implementation scan to verify resolution* – Once the change is implemented; a rescan for the vulnerability will commence to verify the resolution was successful. If the vulnerability is still present, another solution may be attempted or alternative compensating controls [will be evaluated] and implemented. In the event there is no solution, it becomes

a risk that would need to be accepted by the AVPDITS or the device removed from the network.

V. Risk Assessment and Prioritization

The University of South Alabama uses the Common Vulnerability Scoring System (CVSS) for all Common Vulnerabilities and Exposures (CVE) provided by the National Vulnerability Database. A priority is placed on patching or mitigating the vulnerability based on these scores and the logical location of the vulnerability within USA's network infrastructure.

Severity is assigned to vulnerabilities by the exposure to the threat and the risk to the IT environment. The scanning software identifies the location of the vulnerability and current activity of the exploited; the vulnerability assigned one of four ratings. Based off the CVSS score, values from 1 through 3 receive a Low rating, values 4 through 6 receive a Medium rating, values 7 through 9 receive a High severity level, and the value of 10 has a severity level of Critical. See Table 1 for more information.

Table 1

Severity	Description	Time for Remediation
Critical	This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise without requiring user interaction. Flaws that require an authenticated remote user, a local user, or an unlikely configuration are not classed as Critical.	10 business days
High	This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to 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.	30 business days
Medium	This rating is given to flaws that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources, under certain circumstances. These are the types of vulnerabilities that could have had a Critical impact or Important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.	60 business days
Low	This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.	At the discretion of the department

VI. Effectiveness Monitoring

In order to ensure the effectiveness of the Vulnerability Management Policy, the Director of Information Security will conduct a monthly scan and brief the AVPDITS of any vulnerabilities that may cause harm to the University of South Alabama's network.