RUL - 70.00.6 - VULNERABILITY MANAGEMENT RULE

Authority: Information Technology	Responsible Office: Information Technology Services
Number:	RUL - 70.00.6 - VULNERABILITY MANAGEMENT RULE
History:	Effective Date: February 22, 2016; Reformatted/Updated March 10, 2016; Revised: May 10, 2016
Related Policies/Sources:	
Contact Info:	Information Technology Services, 919-530-7423

1. Purpose

The purpose of this rule is to define the requirements for notification, testing, and installation of security-related patches on devices connected to North Carolina Central University’s networks.

2. Rule

2.1 The Chancellor authorizes Information Technology Services (ITS) to conduct routine scans of devices connected to the University networks to identify operating system and application vulnerabilities on those devices as they deemed fit.

2.2 ITS shall ensure that all current maintenance and security vulnerability patches are routinely reviewed the results of vulnerability scans and evaluate, test and mitigate operating system and application vulnerabilities appropriately, as detailed in the Vulnerability Management Process. In addition, only essential application services and ports are enabled and opened in the system’s firewall.

3. Scope

This rule applies to all departments and schools of NCCU. The policy applies to all electronic devices connected to NCCU’s networks (public and private) including but not limited to computer workstations and servers, network switches and routers, specialized laboratory equipment, etc.

4. Rule Enforcement

4.1 The administrators or the owners of the computers and/or servers will comply with this rule to ensure a secure implementation of systems and applications is a critical part of school’s overall information security strategy.

4.2 Administrators and/or owners will be notified of the vulnerabilities report via email (from security@nccu.edu) and the actions that need to be taken. Below is a chart that shows the measures that need to be carried out without delay. The reports will be proposed a resolution to address identified vulnerabilities, required tasks necessary to affect changes, and the assignment of the required tasks to appropriate personnel.

4.3 Vulnerability exceptions are permitted in rare and approved cases whereas a vulnerability has been identified but a patch is not currently available. When a vulnerability risk is “critical impact” or “high impact” and no patch is available, steps must be taken to mitigate the risk through other methods (e.g., workarounds, firewalls, router access control lists). A patch needs to be applied when it becomes available.

4.4 When a “critical impact” or “high impact” vulnerability cannot be totally mitigated within the requisite time frame, administrators and/or owners will need to notify ITS security department by email security@nccu.edu or itscommunication@nccu.edu and call the helpdesk 919-530-7676 of the condition within 2 hours of the “standard required mitigation” was due. There will be a confirmation email sent out. The due dates clock begins when the vulnerabilities report(s) are sent out. Failure to comply with any or all of the vulnerability management policy is subject to ejection from the NCCU’s network without notice.

Impact	**Risk Level on Assessment**	**Standard Required Mitigation**
Critical Impact: could allow exposure/compromise of Secret Information or massive denial or disruption of service	Risk Level **#5 Urgent**	**Within 1 business day**
High Impact: could lead to a compromise of the network(s) and systems(s) if not addressed and remediated within the established timeframe.	Risk Level **#4 Critical**	**Within 7 business day**
Medium Impact: could allow a more limited liability of confidential Information. There is urgency because of a broad exposure.	Risk Level #3 *Serious*	Within 14 days
Low Impact: with a limited of Information being compromise or denial or disruption of service	Risk Level #2 Medium or #1 Minimal	Within 30 days

5. **Vulnerability Levels**

A Vulnerability is a design flaw or misconfiguration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI-bins. Depending on the level of the security risk, the successful exploitation of the vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

6. **Severity Level Description**

6.1 Minimal Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

6.2 Medium Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

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

6.4 Critical Intruders can possibly gain control of the host, 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 host.

6.5 Urgent Intruders can easily gain control of the host, 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.

7. **Potential Vulnerability Levels**

Potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

8. **Severity Level Description**

8.1 Minimal If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities

8.2 Medium If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

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

8.4 Critical If this vulnerability exists on your system, intruders can possibly gain control of the host, 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 host.

8.5 Urgent If this vulnerability exists on your system, intruders can easily gain control of the host, 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.

9. **Information Gathered**

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

10. **Severity Level Description**

10.1 Minimal Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.

10.2 Medium Intruders may be able to determine the operating system running on the host, and view banner versions.

10.3 Serious Intruders may be able to detect highly sensitive data, such as global system user lists.