VSC INFORMATION TECHNOLOGY SERVICES

Patch Application Policy – 1/24/07

Goal

It is the responsibility of each user—both individually and within the organization—to ensure prudent and responsible use of computing and network resources. It is the responsibility of VSC IT to provide a secure network environment for all VSC students, faculty, staff, and business partners. As part of this goal, it is the policy of VSC IT to ensure all VSC-owned computer devices (including servers, desktops, printers, etc.) connected to the VSC network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed.

Scope

This policy covers patches, virus protection software, and operating system updates. Service pack upgrades may be included at the discretion of the local Chief Technology Officer.

Network Administrators Responsibility

The local and system Network Administrators (NetAdmins) and System Administrators are responsible for the overall patch management implementation, operations, and procedures. While safeguarding the network is every user's job, NetAdmins is the group that ensures all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. This responsibility includes the tasks detailed below.

Monitoring

NetAdmins will take prudent steps to monitor security mailing lists, review vendor notifications and Web sites, and research specific public Web sites for the release of new patches. Monitoring may include, but not be limited to, the following: scanning the VSC network to identify known vulnerabilities, identifying and communicating identified vulnerabilities and/or security breaches to CTO's and the CIO, monitoring CERT, SANS notifications, and Web sites of all vendors that have hardware or software operating on the VSC network.

Review, assessment, and testing

If an automated patching mechanism (i.e. WSUS) is not in place, once alerted to a new patch, NetAdmins will download and review the patch within four working hours. NetAdmins will categorize the criticality of the patch according to the following. Not all patches will be applicable to every environment. In assessing the criticality of an applicable patch, NetAdmins may increase the vendor's assessment of criticality, but may not decrease that assessment.

Emergency — an imminent threat to the VSC network
Critical — targets security vulnerability
Not critical — a standard patch release update
Deferrable
Not applicable to the environment

Regardless of platform or criticality, all non-automated patch releases will follow a defined process for patch deployment that includes risk assessment, testing (if necessary based on the risk assessment), scheduling, installing, and verifying.

If any NetAdmin categorizes a patch as an Emergency, IT considers it an imminent threat to the VSC network. In this case, IT assumes a greater risk by not implementing the patch than waiting to test it before implementing. Prudence dictates that emergency patches be applied as quickly as possible.

Notification, scheduling and implementation

IT staff will determine when it is necessary to notify users. NetAdmins will deploy an emergency patch within eight working hours of being alerted to its availability. Patching methods will use the official software update management software from the vendor, such as Microsoft's WSUS system for Windows, and yum or up2date for Linux. For new network devices, each platform will follow established hardening procedures to ensure the installation of the most recent patches.

Auditing, assessment, and verification

Following the release of all patches, NetAdmins staff will verify the successful installation of the patch and that there have been no adverse effects. NetAdmins will also document all exceptions to the patch policy.

References:

VSC Incident Response Policy