Computer Vulnerability Management Practice

1. Purpose

Montana State University is committed to ensuring a secure computing environment and recognizes the need to prevent and manage IT Computer vulnerabilities. A compromised computer threatens the integrity of the network and all computers connected to it. Computer vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within computers in an organization. Proactively managing computer vulnerabilities will reduce or could eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation has occurred.

The purpose of this policy is to ensure that all university-owned computers are proactively managed and patched with appropriate security updates.

Back to Top

2. Definitions

Computer: For the purposes of this practice "Computer" is defined as end-user devices e.g. mobile devices (*excluding phones)*, laptops, and desktops. This excludes any personal (BYOD) device which may be connected to the University network.

Computer Vulnerability Management: Computer vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within Computers in an organization.

Enforced Restart: A restart performed on a user's system by a member of the IT community.

Enterprise Technology Management Policy: Board of Regents policies governing the use of university information technology which apply to all University faculty, staff, students, and patrons. http://www.montana.edu/policy/enterprise_it/technology_management.html

Out-of-band Patch: An emergency software or operating system patch that is being deployed immediately and prior to the next routine restart, usually driven by a zero-day vulnerability exploit.

Patch: Software and Operating System patches normally fix bugs, but they can also be released to address security vulnerabilities and inconsistencies in a piece of software. Skipping over these important updates can leave your computer, phone, or another device open to malware attacks that the patch is intended to prevent.

Patch Applied: Refers to a patch that was deployed and has been applied to a computer or software, usually requiring a restart of the computer to activate the software or computer patch.

Patch Deployment: Refers to a patch that has been delivered to a computer, but not applied.

Restart: A restart is the process of restarting a working computer. Restarting is sometimes necessary after installing a computer or software patch.

Technology Management Standards: Standards established as a minimum guideline for management of devices connecting to MSU's network as outlined in the University Technology Management Policy. http://www.montana.edu/uit/security/documents/Technology-Management-Standards.pdf

University-owned Computer: For the purposes of this practice a "University-Owned Computer" is defined as any computer which was purchased using funds managed by the university, including grants. These computers include but are not limited to, any laptop or workstation which was deployed to faculty or staff. This excludes any personal (BYOD) device which may be connected to the university network.

Update: An update does not specifically address critical security issues and is usually focused on adding additional functionality and features to the software or operating system. An update could include a fix to address a security issue.

Vulnerability: A security hole in software, such as browser software or operating system software.

Zero-Day Exploit: Code that attackers use to take advantage of a zero-day vulnerability. If we see or hear of cyber criminals exploiting a zero-day vulnerability, UIT will test, and then install the appropriate patch to computers as soon as it becomes available.

Back to Top

3. Scope

This policy applies to all university owned computer that may connect to the University network

Back to Top

4.0 Procedures

4.0.1 Scheduling, Deployment and Application

4.0.2 Scheduling

Standing practice will be to restart all computers weekly between 10:00 p.m. Wednesday night and 3:00 a.m. Thursday morning. This will ensure all computer patches are applied on a regular scheduled. Except for those computers that have been opted out of a weekly restart.

An unscheduled restart of a computer, prior to the next routine restart, may be required to address a zero-day exploit. This may be needed to ensure the out-of-band patch is applied and can prevent the computer from being exploited. In the event that an unscheduled restart is needed, communication will be sent to all users' @montana.edu email addresses advising that UIT will be performing an unscheduled restart and the date the restart will begin. Computers will then be restarted on the specified date, that night between 10:00 p.m. and 3:00 a.m. the next morning.

Release of patches occurs on a varying scheduled dependent on the software or operating computer vendor, therefore no set schedule is available per vendor.

4.0.3 Deployment

Applicable patches will be tested and validated by UIT prior to deployment to campus.

Once validated, UIT will schedule and deploy validated patches on an as needed basis.

4.0.4 Application & Restart

Once a patch is applied to an operating system or software, a restart of a computer may be required to successfully install most security patches.

Until the restart occurs, the computer remains vulnerable to attacks which the installed patch protects against.

Standing practice will be to restart all Computers weekly between 10:00 p.m. Wednesday night and 3:00 a.m. Thursday morning. This will ensure all patches and/or updates are applied on a regular scheduled. Except for those computers that have been opted out of a weekly restart.

Back to Top

4.1 Out-of-Band Patch/Update

On occasion a software or systems vendor will release a highly critical security patch/update outside of their normal release cycle.

The usual reason for the release of an out-of-band patch/update is the appearance of a zero-day vulnerability exploit.

An unscheduled restart of a computer, prior to the next routine restart, may be required to address a zero-day exploit. This may be needed to ensure the out-of-band patch/update is applied and can prevent the computer from being exploited.

In the event that an unscheduled restart is needed, communication will be sent to all users' @montana.edu email addresses advising that UIT will be performing an unscheduled restart and the date the restart will begin. Computers will then be restarted on the specified date, that night between 10:00 p.m. and 3:00 a.m. the next morning.

Back to Top

4.2 Restart Exemption

There is the possibility of academic or administrative processes being negatively impacted by a computer restart.

Users who manage computers that could be impacted by a computer restart, can fill out the Restart Exemption Request form located

www.montana.edu/uit/computing/desktop/cvm/restart_exempt_request.html and request to be temporarily exempted from that week's mandatory restart process.

These requests must be submitted by 3:00 p.m. Tuesday each week.

Each request will be reviewed on a case by case basis and will only apply for the next scheduled patch.

After the exemption has passed, the computer will resume the normal patch restart schedule. That means the computer will be restarted the following Wednesday, between 10:00 p.m. Wednesday night and 3:00 a.m. Thursday morning.

If a computer you manage, needs to be exempted from a restart beyond the next scheduled patch please contact the UIT Service Desk directly. This type of exemption will be evaluated by your manager and UIT.

Restart exemptions **DO NOT APPLY** to out-of-band patches.

Back to Top

4.3 Out-of-Band Restart Exemption

Due to the highly critical nature of an out-of-band patch/update and the associated appearance of a zero-day vulnerability exploit, exemptions are not available for out-of-band patches.

Back to Top

4.4 Computer Vulnerability Management – Permanent Opt Out

If you feel a computer you manage should never receive any system updates or patches, please contact the UIT Desk directly by 3:00 p.m. Tuesday the week you wish your exemption to begin. Requests for permanent exemptions will be evaluated by your manager and UIT.

Back to Top

4.5 Updates vs. Patching

A Software and/or Operating System **PATCH** normally fixes bugs, but they can also be released to address security vulnerabilities and inconsistencies in a piece of software.

An **UPDATE** does not specifically address critical security issues and is usually adding additional functionality and features to the software or operating system.

Back to Top