

UMB, UMMC, UPI, and SOM Microsoft Windows Operating System Patch Management Policy

Executive Summary

The Windows Operating System (WOS) contains flaws. Occasionally, one of those flaws permits a hacker to compromise a computer running a WOS. A compromised computer threatens the integrity of the network and all computers connected to it. Therefore, computer equipment that runs WOS and is connected to the campus network must have up-to-date critical security patches applied.

Goal

To ensure all WOS systems do not pose an unmanaged security risk for the campus, by ensuring applicable and required security patches for WOS are applied in a timely and effective manner. To define campus standards for auditing, reporting, communication, and contingency planning in regards to the management of WOS security patches.

Scope

This policy applies to every WOS workstation physically (including wireless) connected to any part of the campus network.

Definitions:

Departmental IT Manager – Individual or group responsible for maintaining Microsoft Windows servers or workstations for an organization and/or department.

Deployment Group – Individual or group responsible for the deployment of Microsoft Windows patches.

General Policy

Operational Guidelines

1. Departmental IT managers must maintain portable media containing copies of the latest Windows client patches for the deployment of new or redeployment of existing PC's. Applicable patches must be installed prior to connecting the computer to the network. Each campus networking group will also maintain copies on portable media.
2. Each campus network group, all campus LAN administrators and Departmental IT Managers must subscribe to Microsoft Security Bulletin email distribution list (http://www.microsoft.com/security/list_subscribe.asp).

Technical Guidelines

1. Current patches for the following Microsoft supported products must be maintained:
 - a. Windows 2000/XP
 - b. Internet Explorer
 - c. Microsoft SQL Server Desktop Engine (MSDE)
 - d. Microsoft Data Access Components (MDAC)
 - e. Microsoft Office Suite
 - f. Outlook
 - g. Windows Media Player
 - h. DirectX
2. Campus network groups, LAN administrators and/or Departmental IT Managers will regularly audit (note: a minimal audit cycle should be recommended – need to include a timeframe for the audit cycle) networked computers to determine the need for security patches. Automatic scanning systems, administered from central sites, are superior to manual patching methods. It must be possible to define scans by:
 - a. IP ranges
 - b. Domain/AD
 - c. Machine Names
3. It must be possible to automatically deploy patches for the Microsoft products listed above from central sites following the same criteria described for scanning.
4. If administrative rights to a computer are necessary requirements for a selected automated patch management system then local creation of and assured access to that account are conditions for continued attachment of that computer to a campus network. Required administrative accounts will follow minimal password standards for authentication. Default passwords will not be allowed.
5. Automated scanning and deployment (patch management) systems must also be able to provide lists of:
 - a. Missing Patches and/or Service Packs
 - b. WOS Versions
 - c. Patches that were successfully applied
 - d. Patches that could not be applied
6. The patch management product employed must store all information in a structured database.

Configuration

Client Configuration

1. Machines will be configured according to the Campus Network Device Naming Convention policy.
2. Clientless systems are preferred. However, if a client-based system is employed, it must be possible to deploy and configure it remotely.

Patch Approval Process

Since a WOS security patch may cause an application to malfunction, departmental IT managers should proactively announce the deployment of a patch(es). It is the responsibility of application owners to identify any problem(s) with a patch(es) and to notify the departmental IT manager of the problem(s). It is also the responsibility of application owners to resolve this incompatibility with the application's maker. If the maker cannot resolve the incompatibility, the risk incurred by not patching the computer(s) in question must be weighed against the risk of not running the application. The department IT manager and the application owner should evaluate the options taking into consideration the nature of the vulnerability, the likelihood of its exploitation and the impact to operations of application malfunction. If they determine that the patch in question should not be deployed, this decision must be communicated to the appropriate CIO.

Deployment

Critical security patches should be deployed within two business days of the time Microsoft makes them available. Non-critical security and other patches may be applied monthly. A roaming workstation must have Windows Automatic Updates configured to automatically download and install patches when it physically (or by wireless) connects to a campus network.

Auditing and Monitoring

1. Post-patch audit scans must occur within 1 week after Microsoft releases a critical security patch.
2. Regular or pre-patch network-wide audit scans must be performed at least monthly.
3. Audit reports must be maintained for at least 1 year.

Contingency Planning

System Failure

1. In the event that a critical patch cannot be centrally deployed, it must be installed in a timely manner either manually or via Windows Automatic Update.
2. One or more alternate central console server administrators must be designated and trained so that in the event the primary administrator, Deployment Group or Departmental IT Manager are not available the patch and audit processes can proceed normally.
3. CDs containing all current patches will be provided to IT managers.

Incident Response and Reporting

Outbreak Management

Campus network administrators will take reasonable and appropriate measures to defend networking functions during malicious attacks. They will apprise their respective CIO about the nature, extent and consequences of the attack and their actions. In turn, the CIO will immediately inform the other campus CIOs about details of the incident.

Communication

General Communication

Digital communications (email and web) may be disrupted during an incident., Use voice or fax on these occasions.

Email – CITS maintains a central email list for important security notifications. Go to <http://www.umaryland.edu/cits/security> and select the Campus IT Security Listserver link.

Broadcast Voice Messages –In extreme circumstances, broadcast voice messaging may be required.

Effective Date

Patch management, as defined in this document, is to begin immediately.

- Workstations will need to be configured according to campus naming standard.

Compliance of this policy should occur no later than July 1, 2004.

Violations

- Failure to properly configure new workstations is a violation of this policy
- Disabling, circumventing or tampering with patch management protections and/or software constitutes a violation of policy.
- It is the responsibility of each departmental IT administrator to make sure that they are keeping their departmental systems in compliance with the above stated policy. Failure to do so constitutes a violation of policy.

Enforcement

Violations in policy could result in progressive disciplinary action dealt with through normal disciplinary processes within each organization.

In the course of monitoring, any computers found not to be in compliance will be disconnected from the network until they can be properly configured.

Revisions

As the nature of threats, vulnerabilities and technologies change, this policy will be reviewed and revised accordingly.

Issues & Considerations:

Campus IT representatives should take time to research and recommend a unified strategy for implementing this patch management policy using central deployment servers. It will be beneficial to have vendors come to campus to demonstrate their products. As with anti-virus software, the aim is to effectively manage diverse campus resources while not requiring a single vendor solution.

Implementing this policy requires funding to purchase enterprise patch management software and perhaps additional hardware. Additional personnel may be required to properly configure workstations and servers.

Workstations on the campus network must be migrated to a supported WOS.. Additional funding may be needed to upgrade or replace those systems.. Failure to do so will create a pool of networked computers that will act as a staging area for future malicious attacks.

Note: there is no policy for proactively managing patches on clinical devices that run the WOS. These devices present a serious risk to the enterprise. A decision must be made as to who has responsibility for maintaining the path levels of these devices.

Grandfather clause – Computers running unsupported WOS software may remain on the campus network until they are upgraded. However, at the first sign of compromise, they will be disconnected from the campus network and will not be reconnected until a supported WOS is installed.