****

|  |  |
| --- | --- |
| Section: | IT |
| Title: | Desktop, Server and Network Patches |
| Effective Date: | 10/1/2013 |
| Approved By: | Information Technology |
| Responsible Unit: | Information Technology |
| History: |  |
| Related Documents: | |

1. **INTRODUCTION**

The purpose of these guidelines is to document the procedure applying operating system patches to desktop computers and servers. While this document serves as a general guide for how regular patches are applied, the College IT has the means to immediately distribute patches to fix the high severity vulnerabilities (a.k.a. zero-day vulnerabilities). The College IT also maintains network-based solutions that allow for “virtual patching” or “network-based patching” that can mitigate the risks for certain vulnerabilities while traditional patches are prepared and distributed.

1. **DEFINITIONS**

None.

1. **STANDARD**

**Microsoft Desktop Workstations**

Microsoft typically releases new patches on the first Tuesday of the month. Information Technology delays the release of Microsoft’s patches in order to all time for trouble reports to appear and be evaluated. IT releases critical and important patches on the following schedule:

Second Tuesday of the month: WSUSTest group (three labs and the USS division)

Fourth Tuesday of the month: the balance of the campus Windows Desktops Workstations

This list below outlines in detail how these patches are deployed to the College owned Microsoft Windows desktop computers.

Patches are deployed via Microsoft Group Policy Objects (GPOs). Those definitions are:

**Microsoft Group Policy Definitions:**

* Allow Automatic Updates immediate installation: Enabled
* Allow signed updates from an intranet Microsoft update service location: Enabled
* Configure Automatic Updates: Enabled
* Configure automatic updating: 4 - Auto download and schedule the install
* Scheduled install day: Everyday (NOTE: this means the workstations are checking for patches everyday. Releases of patches follows the above schedule.)
* Scheduled install time: 11:00
* Delay Restart for scheduled installations: Enabled (15 minutes for faculty/staff, 30 minutes for labs)
* Wait the following period before proceeding with a scheduled restart (minutes): 15
* Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box: Enabled
* Enable client-side targeting: Enabled
* Target group name for this computer: §1
* Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates: Enabled
* Re-prompt for restart with scheduled installations: Enabled
* Wait the following period before prompting again with a scheduled restart (minutes): 10
* Reschedule Automatic Updates scheduled installations: Enabled (15 minutes)
* Wait after system startup (minutes): 15
* Specify intranet Microsoft update service location: Enabled (10 minutes)
* Set the intranet update service for detecting updates: http://wsus.tcnj.edu
* Set the intranet statistics server: http://wsus.tcnj.edu
* Turn on recommended updates via Automatic Updates: Enabled
* Allow non-Administrators to receive update notifications: Enabled
* Turn on software notifications: Enabled
* Automatic Updates Detection Frequency: Enabled (20 hours)
* No auto-restart with logged on users for scheduled automatic updates installations: Enabled

**§1 – Value will be one of the following:**

* Lab
* Staff
* WSUSTest
* WSUSOptout

**WSUS Group Pairings:**

* Lab contains all Windows Desktop lab computers not found in WSUSTest
* Staff contains all faculty and staff computers not found in WSUSTest
* WSUSTest contains computers in the USS division, Library labs 2 and 5, and Social Sciences 21
* WSUSOptout contains any computers that should not receive patches for reasons of compatibility, useability, or other reasons.

**Microsoft Servers**

Because the College IT operations is a 24x7 operation, care must be taken when updating servers so as not to unnecessarily disrupt operations due to a bad patch or required server reboot.

The Microsoft Windows server patches are maintained and pushed via a separate WSUS server from the Windows desktop patches.

For all servers, patches will be downloaded to the server but updates may be automatic or manual depending on the type of server.

Microsoft infrastructure servers (e.g. Active Directory, DNS, file and print servers) will receive critical and security patches automatically via the WSUS server.

For Microsoft application servers, critical patches are evaluated on a per server basis to make sure it will not cause operational issues. The 3rd party software vendor may also need to be consulted to make sure it is supported by their software. The system administrator will schedule and manually apply patches to these servers.

The goal is to make sure all critical and security patches are applied in a timely fashion to servers. Some patches, such as for zero-day attacks, may require immediate patching and server reboots that may be disruptive but necessary to maintain the security of the TCNJ network and server infrastructure.

Less critical patches and system enhancement patches are evaluated and applied during normal breaks in the college operations. These include the summer months, winter break, spring break and fall break.

**Apple Mac Desktops**

It is left to the end-user and IT Support Specialist (for labs) to apply patches to Mac desktops. The Mac OS will identify patches available from Apple and request that the end-user apply the updates to their desktop.

**Red Hat Enterprise Linux (RHEL) Servers**

Similar to the Microsoft Windows server process, the College has a Red Hat Network (RHN) Satellite server installed. This allows IT to have a local cache of patches and the ability to review the patches and deploy to servers.

RHEL servers patches are deploy during normal breaks in the college operations. These include the summer months, winter break, spring break and fall break.

Critical and security patches are evaluated scheduled and deployed as necessary between the college breaks. Special attention is paid to Internet accessible servers and those that appear on the regular vulnerability scans that are performed monthly.

**Network Devices**

Patches to network devices are evaluated monthly and scheduled appropriately. Critical security related patches are scheduled and deployed as soon as reasonably possible. Patches that provide bug fixes or new features are evaluated with the vendor to determine their impact to our network, and scheduled so that there is minimal impact to the campus community.

1. **RELATED DOCUMENTS**
2. **HISTORY**