BCU Patching Summary

Created 8/03/2023 Ver 4.0 Last Updated 8/23/2024

Summary

There are five systems involved. Four systems for delivering patches to our end points and a fifth for identifying and reporting vulnerabilities.

- Microsoft System Center Configuration Manager (MECM) for Domain joined PCs and some servers and Azure Update Manager for remaining servers
- Microsoft Intune: Laptops and other off network resources, including phones & tablets
- Jamf: Macs
- Qualys: Vulnerability scanning, reporting & tracking

Individuals responsible for the Patch Management Process

Systems Engineering and Platform Engineering teams are responsible for patching all BCU devices.
System Engineering is responsible for patching Desktops (Domain and non Domain Joined), laptops, Macs and servers using MECM, Intune and Jamf. Platform Engineering uses Azure Update manager

Patches are provided by the various manufacturers at different times, depending on the release schedule from that manufacture. However, BCU operates patching monthly on a 4-week cycle starting with the weekend after Microsoft's Patch Tuesday (second Tuesday of the calendar month).

Patch Management Schedule

Patches that are applied and pending reboots between the hours of 2:00 p.m. CST on Saturday and 4:00 a.m. CST Sunday.

PATCH ZONE DEFINITION

Zone A (Azure) - Development servers & a small number of IT VMs
Zone B (Azure) – Half of production, dividing up each environment to avoid patching all at same time
Zone C (Azure) – Other Half of production, dividing up each environment to avoid patching all at same time.
Zone 4 (SCCM) Zone M(Azure) - Manual patching zone for servers. narrow maintenance windows or requires rebooting manually. e.g., Nutanix hosts.
Zone 5 (SCCM) - Fedline Machines that require a different schedule than any other zone.
SQL Prod

MECM and Azure PATCH Management Cycle

2nd Tuesday of the month	Microsoft Releases Patches (COTS patches obtained)
2nd Wednesday of the month	ADR in SCCM runs at 2:00 a.m. downloading patches Zone 4, Zone 5 and SQL Prod for SCCM are made available for owners of the manual patching servers to install
1st Saturday after Patch Tues	Zone A
2nd Saturday after Patch Tues	Zone B
3rd Saturday after Patch Tues	Zone C
4th Saturday after Patch Tues	All zone remediation

Intune PATCH Management Cycle

Windows Update Ring phases

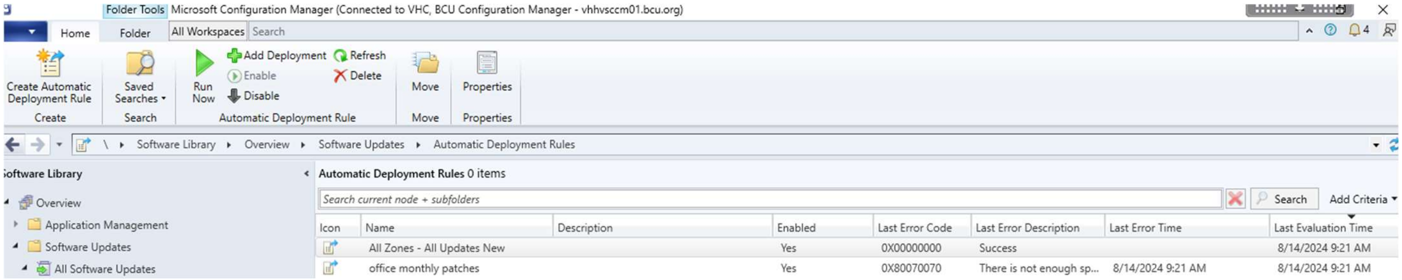
Phase 1: The "IT Focus Group" laptop testers and "Branch Desktop" device test group receive the new releases on Patch Tuesday on day 1. They're instructed to report any strange behavior after the patch is installed.
Phase 2: Patches will deploy to all production machines enrolled in Intune. The user will receive an alert to initiate the install and reboot for two days. On the third day, the reboot is enforced to finalize the update.

Microsoft Endpoint Configuration Manager (MECM)

For patch deployment on Workstations (specifically domain joined desktops) and Servers, MECM is used as a centralized deployment tool, and we use the same for the management of patch lifecycle in the environment. To manage patching we use the Software Updates module of MECM. Every month on the second Tuesday Microsoft releases patches for all the Windows operating system and other products such as MS office etc.

Automatic Deployment Rules (ADRs)

MECM uses **A**utomatic **D**eployment **R**ules (ADRs) to query Microsoft each month on Patch Tuesday and pull down the required patches. The downloaded patches are automatically bundled into Deployment Packages for distribution to the End Points based on the schedule in this document.



Microsoft Configuration Manager (Connected to VHC, BCU Configuration Manager - vhhvsccm01.bcu.org)

Automatic Deployment Rules 0 items

Icon	Name	Description	Enabled	Last Error Code	Last Error Description	Last Error Time	Last Evaluation Time
	All Zones - All Updates New		Yes	0X00000000	Success		8/14/2024 9:21 AM
	office monthly patches		Yes	0X80070070	There is not enough sp...	8/14/2024 9:21 AM	8/14/2024 9:21 AM

We additionally pull-down patches from various third-party manufacturers, for their “Commercial Off The Shelf (COTS) packages such as Google Chrome, Mozilla Firefox, Adobe Reader, etc. Depending on the manufacturer, this process may be manual or automated with SCCM. These updates are applied with change tickets when necessary, depending on vulnerability criticality identified by Qualys.

SQL Prod Servers

MECM makes the patches available to run via Software Center manually on the day after Patch Tuesday. This is to control the timing of the install and control reboot due to the sensitivity of these specific machines. SQL team at this time controls when it installs.

Qualys

Qualys vulnerability scans are performed periodically weekly by the security team. The result of the weekly scan is provided to the Systems Engineering team and the Platform Engineering team via individual emailed reports for each category of devices (Server, Desktop, Laptops, etc). The weekly scan is also provided in a shared spreadsheet (see example below) which teams can use to assign out work. The output from these scans are used to target devices and additional patches that may be missing or have not been fully remediated through the monthly patching processes. Any issues identified are then remediated using the tools above.