Discussion-5 Third-party applications vulnerabilities

Discussion Topic:

Select two third-party applications (not OSs) that you frequently use. How does each of them address patch management? Visit their websites to determine how they alert users to new vulnerabilities. Are the patch management systems adequate? Provide your thoughts on the advantages and disadvantages if patch management were required for all third-party applications.

My Post:

Hello Class,

Two third-party applications that I use daily are Microsoft Word and Google Chrome.

Microsoft Word is part of the Microsoft 365/Office application suite. The Microsoft 365 Apps updates/patches for Mac are part of the Microsoft AutoUpdate (MAU) (Microsoft Ignite, 2025a). MAU is a utility software that is designed to keep Microsoft applications up-to-date (patch-up) on macOS (Microsoft Ignite, 2024b). They patch the application as soon as a vulnerability is identified. I use Microsoft 365 Apps on a Windows system.
Microsoft alerts users about new vulnerabilities using communication bulletins and linking them to their corresponding patches. These bulletins and the corresponding patches are managed by the Microsoft Security Response Center (MSRC) (Gallagher, 2025). For consumer and unmanaged devices, the updates are performed automatically using Windows Update, that is, ─if receive updates for Microsoft products when you update Windows is enabled─, these updates include Office. Microsoft also alerts users directly when sensitive, urgent security updates are needed, by prompting the user to update their system immediately (to restart their devices). For business devices and managed devices, Microsoft provides a suite of management tools, such as Microsoft Configuration Manager (SCCM), to configure Microsoft apps and their updates (Wiland, 2022).
In my opinion, these measures, their patch management systems, are adequate. Especially, the Microsoft 365 patch management system is considered excellent as it provides flexible update, automated deployment options (like Click-to-Run and Windows Autopatch for enterprise environments), and robust control for IT administrators to manage update cadences, test patches, and ensure compliance across an organization's devices, significantly reducing the attack surface and enhancing overall system stability and security.

Google Chrome is automatically updated/patched by using Google Update on Windows and on macOS systems (Google Support, n.d.a). These updates are designed to protect users from the latest web-based threats through minimal user involvement. Google does not directly alert users when Chrome needs an update; instead, it handles security updates through rapid and automatic patching. Usually, the application will prompt the user to relaunch it when an update is available. For enterprise environments, Google provides Chrome update control/management through Group Policy settings (for Windows) or Google Software Update (for macOS) (Google Support, n.d.b; Google Support, n.d.c).
In my opinion, these measures to patch Chrome are adequate. This automatic and rapid implementation of security updates ensures that users are running secure versions (most of the time) of the application. It is a “set it and forget it” approach that protects from common/known web-based threats.

I think that mandatory patch management for all third-party applications has many advantages; it can benefit these applications' security by reducing the number of known exploitable vulnerabilities and the capacity of attackers to exploit new/unknown vulnerabilities. However, significant practical challenges (disadvantages) exist, such as implementation, compatibility, and resource allocation issues, that may make mandatory patch management for all third-party applications very difficult for individual users and organizations.

-Alex

References:

Gallagher, T. (2025, March 13*). How MSRC coordinates vulnerability research and disclosure while building community*. Microsoft. https://www.microsoft.com/en-us/security/blog/2025/03/13/how-msrc-coordinates-vulnerability-research-and-disclosure-while-building-community/#:~:text=Security%20operations-,more,a%20responsible%20and%20timely%20manner.

Google Support (n.d.A). *Update Google Chrome*. Google. https://support.google.com/chrome/answer/95414?hl=en&co=GENIE.Platform%3DDesktop

Google Support (n.d.b). Manage Chrome updates (Windows). Google. https://support.google.com/chrome/a/answer/6350036?hl=en#:~:text=Step%202%3A%20Configure%20auto%2Dupdates,apps%20managed%20by%20Google%20Update.

Google Support (n.d.c). Manage Chrome updates (Mac). Google. https://support.google.com/chrome/a/answer/7591084?hl=en

Microsoft Ignite (2025a, April 22). Microsoft 365. *Release history for Microsoft AutoUpdate (MAU)*. Microsoft Learn. https://learn.microsoft.com/en-us/officeupdates/release-history-microsoft-autoupdate

Microsoft Ignite (2024b, September 18). Microsoft 365. Deploy updates for Office for Mac. Microsoft Learn. https://learn.microsoft.com/en-us/microsoft-365-apps/mac/deploy-updates-for-office-for-mac

Wieland, M. (2022, September 1). *Microsoft configuration manager overview*. Recast Software. https://www.recastsoftware.com/resources/configmgr-sccm-overview/