Microsoft: Happy 2025. Here’s 161 Security Updates

January 14, 2025 27 Comments

Microsoft today unleashed updates to plug a whopping 161 security vulnerabilities in **Windows** and related software, including three “zero-day” weaknesses that are already under active attack. Redmond’s inaugural Patch Tuesday of 2025 bundles more fixes than the company has shipped in one go since 2017.

Rapid7's **Adam Barnett** says January marks the fourth consecutive month where Microsoft has published zero-day vulnerabilities on Patch Tuesday without evaluating any of them as critical severity at time of publication. Today also saw the publication of nine critical remote code execution (RCE) vulnerabilities.

The Microsoft flaws already seeing active attacks include CVE-2025-21333, CVE-2025-21334 and, you guessed it– CVE-2025-21335. These are sequential because all reside in **Windows Hyper-V**, a component that is heavily embedded in modern **Windows 11** operating systems and used for security features including device guard and credential guard.

Tenable's **Satnam Narang** says little is known about the in-the-wild exploitation of these flaws, apart from the fact that they are all "privilege escalation" vulnerabilities. Narang said we tend to see a lot of elevation of privilege bugs exploited in the wild as zero-days in Patch Tuesday because it's not always initial access to a system that's a challenge for attackers as they have various avenues in their pursuit.

"As elevation of privilege bugs, they're being used as part of post-compromise activity, where an attacker has already accessed a target system," he said. "It's kind of like if an attacker is able to enter a secure building, they're unable to access more secure parts of the facility because they have to prove that they have clearance. In this case, they're able to trick the system into believing they should have clearance."

Several bugs addressed today earned CVSS (threat rating) scores of 9.8 out of a possible 10, including CVE-2025-21298, a weakness in Windows that could allow attackers to run arbitrary code by getting a target to open a malicious **.rtf** file, documents typically opened on Office applications like Microsoft Word. Microsoft has rated this flaw "exploitation more likely."

Ben Hopkins at **Immersive Labs** called attention to the CVE-2025-21311, a 9.8 "critical" bug in **Windows NTLMv1** (NT LAN Manager version 1), an older Microsoft authentication protocol that is still used by many organizations.

"What makes this vulnerability so impactful is the fact that it is remotely exploitable, so attackers can reach the compromised machine(s) over the internet, and the attacker does not need significant knowledge or skills to achieve repeatable success with the same payload across any vulnerable component," Hopkins wrote.

Kev Breen at Immersive points to an interesting flaw (CVE-2025-21210) that Microsoft fixed in its full disk encryption suite **Bitlocker** that the software giant has dubbed "exploitation more likely." Specifically, this bug holds out the possibility that in some situations the hibernation image created when one closes the laptop lid on an open Windows session may not be fully encrypted and could be recovered in plain text.

"Hibernation images are used when a laptop goes to sleep and contains the contents that were stored in RAM at the moment the device powered down," Breen noted. "This presents a significant potential impact as RAM can contain sensitive data (such as passwords, credentials and PII) that may have been in open documents or browser sessions and can all be recovered with free tools from hibernation files."

Tenable's Narang also highlighted a trio of vulnerabilities in **Microsoft Access** fixed this month and credited to Unpatched.ai, a security research effort that is aided by artificial intelligence looking for vulnerabilities in code. Tracked as CVE-2025-21186, CVE-2025-21366, and CVE-2025-21395, these are remote code execution bugs that are exploitable if an attacker convinces a target to download and run a malicious file through social engineering. Unpatched.ai was also credited with discovering a flaw in the December 2024 Patch Tuesday release (CVE-2024-49142).

"Automated vulnerability detection using AI has garnered a lot of attention recently, so it's noteworthy to see this service being credited with finding bugs in Microsoft products," Narang observed. "It may be the first of many in 2025."

If you're a Windows user who has automatic updates turned off and haven't updated in a while, it's probably time to play catch up. Please consider backing up important files and/or the entire hard drive before updating. And if you run into any problems installing this month's patch batch, drop a line in the comments below, please.

Further reading on today's patches from Microsoft:

Tenable blog

SANS Internet Storm Center

Ask Woody

This entry was posted on Tuesday 14th of January 2025 05:50 PM

LATEST WARNINGS | THE COMING STORM | TIME TO PATCH

ADAM BARNETT BEN HOPKINS BITLOCKER CVE-2024-49142 CVE-2025-21186 CVE-2025-21210 CVE-2025-21298 CVE-2025-21311 CVE-2025-21333 CVE-2025-21334 CVE-2025-21335 CVE-2025-21366 CVE-2025-21395 KEV BREEN MICROSOFT ACCESS MICROSOFT PATCH TUESDAY JANUARY 2025 RAPID7 SATNAM NARANG UNPATCHED.AI WINDOWS 11 WINDOWS HYPER-V WINDOWS NTLMV1

27 thoughts on "Microsoft: Happy 2025. Here's 161 Security Updates"

Oliver

January 14, 2025

Based on the wording from Microsoft, CVE-2025-21298 doesn't appear to require users to actually open the RTF files as currently-worded in this article (such as those that arrive as an email attachment). The vulnerability seems to be related to OLE such that Outlook is affected, so all the attacker needs to do is send a specially-crafted email to a target that uses Outlook. This is a somewhat important distinction (specific user interaction not being required) and I believe is part of why it's rated at a 9.8.

Uncle Jack

January 14, 2025

Speaking of Microsoft, there is a current article about some dodgy code in the 6.13 kernel submitted by a Microsoft engineer that could have caused serious issues with some systems.

Happy Jack

-

January 14, 2025

A funny headline about the issue: "Microsoft pulls a Windows as it breaks Linux on Intel CPUs and angers AMD in the process"

- Catwhisperer

-

January 18, 2025

I just bought a Lenovo neo 50t. It runs Ubuntu Pro 24.04, but sometimes it has to by force when it comes to Windows. It is a dual boot machine, with Windows 11 Pro on another partition. On install, and now apparently on Update Tuesday, 11 Pro decides to diddle with the boot sequence in UEFI and place itself first. That forces me to go back into UEFI and change the boot sequence. Even with a supervisor password on UEFI.