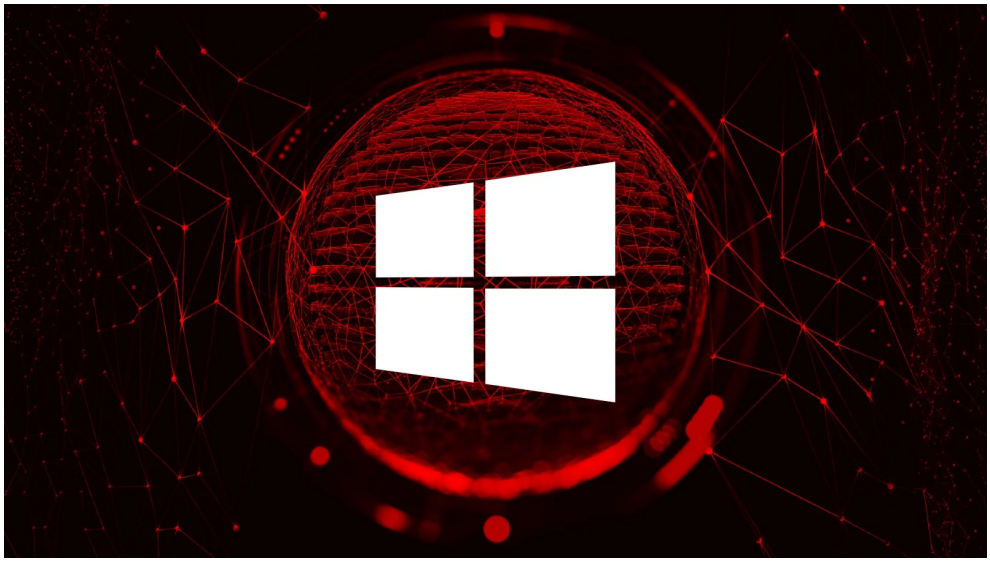
Microsoft releases emergency fixes for Windows Server, VPN bugs

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** January 17, 2022 05:46 PM **6**



Microsoft has released emergency out-of-band (OOB) updates to address multiple issues caused by Windows Updates issued during the January 2021 Patch Tuesday.

"Microsoft is releasing Out-of-band (OOB) updates today, January 18, 2022, for some versions of Windows," the company said.

"This update addresses issues related to VPN connectivity, Windows Server Domain Controllers restarting, Virtual Machines start failures, and ReFS-formatted removable media failing to mount."

All OOB updates released today are available for download on the Microsoft Update Catalog (https://www.catalog.update.microsoft.com/Home.aspx), and some of them can also be installed directly through Windows Update as optional updates.

You will have to manually check for updates if you want to install the emergency fixes through Windows Update because they are optional updates and will not install automatically.

The following updates can only be downloaded and installed via the Microsoft Update Catalog:

- Windows 8.1, Windows Server 2012 R2: KB5010794 (https://support.microsoft.com/help/5010794)
- Windows Server 2012: KB5010797 (https://support.microsoft.com/help/5010797)

Updates for these Windows versions are also available through Windows Update as an optional update:

- Windows 11, version 21H1 (original release): KB5010795 (https://support.microsoft.com/help/5010795)
- Windows Server 2022: KB5010796 (https://support.microsoft.com/help/5010796)
- Windows 10, version 21H2: KB5010793 (https://support.microsoft.com/help/5010793)
- Windows 10, version 21H1: KB5010793 (https://support.microsoft.com/help/5010793)

- Windows 10, version 20H2, Windows Server, version 20H2: KB5010793 (https://support.microsoft.com/help/5010793)
- Windows 10, version 20H1, Windows Server, version 20H1: KB5010793 (https://support.microsoft.com/help/5010793)
- Windows 10, version 1909, Windows Server, version 1909: KB5010792 (https://support.microsoft.com/help/5010792)
- Windows 10, version 1607, Windows Server 2016: KB5010790 (https://support.microsoft.com/help/5010790)
- Windows 10, version 1507: KB5010789 (https://support.microsoft.com/help/5010789)
- Windows 7 SP1: KB5010798 (https://support.microsoft.com/help/5010798)
- Windows Server 2008 SP2: KB5010799 (https://support.microsoft.com/help/5010799)

January Windows updates issues and fixes

As BleepingComputer reported after this month's Patch Tuesday (https://www.bleepingcomputer.com/news/microsoft/new-windows-server-updates-cause-dc-boot-loops-break-hyper-v/), the latest Windows Server updates were causing a series of severe issues for administrators.

According to admin reports, Windows domain controllers were being plagued by spontaneous reboots, Hyper-V was no longer starting on Windows servers, and Windows Resilient File System (ReFS) volumes were no longer accessible after deploying the January 2021 updates.

Windows 10 users and administrators also reported problems with L2TP VPN connections after installing the recent Windows 10 and Windows 11 cumulative updates and seeing "Can't connect to VPN." errors.

Those who cannot immediately install today's out-of-band updates can remove the KB5009624, KB5009557, KB5009555, KB5009566, and KB5009543 updates causing these issues from an Elevated Command Prompt (https://www.bleepingcomputer.com/tutorials/how-to-open-a-windows-10-elevated-command-prompt/) with the following commands:

```
Windows Server 2012 R2: wusa /uninstall /kb:KB5009624
Windows Server 2019: wusa /uninstall /kb:KB5009557
Windows Server 2022: wusa /uninstall /kb:KB5009555
Windows 10: wusa /uninstall /kb:5009543
Windows 11: wusa /uninstall /kb:5009566
```

However, since Microsoft also bundles all the security updates with these Windows cumulative updates, removing them will also remove all fixes for vulnerabilities patched during the January 2021 Patch Tuesday.

Windows admins and users need to consider the risks of unpatched vulnerabilities impacting their systems versus the disruption caused by the issues stemming from this month's Windows updates.

Related Articles:

Windows 'RemotePotato0' zero-day gets an unofficial patch (https://www.bleepingcomputer.com/news/security/windows-remotepotato0-zero-day-gets-an-unofficial-patch/)

Microsoft: New critical Windows HTTP vulnerability is wormable (https://www.bleepingcomputer.com/news/microsoft/microsoft-new-critical-windows-http-vulnerability-is-wormable/)

Microsoft increases Windows 11 rollout pace to Windows 10 devices (https://www.bleepingcomputer.com/news/microsoft/microsoft-increases-windows-11-rollout-pace-to-windows-10-devices/)

Emergency Windows Server update fixes Remote Desktop issues (https://www.bleepingcomputer.com/news/microsoft/emergency-windows-server-update-fixes-remote-desktop-issues/)

Malware now trying to exploit new Windows Installer zero-day (https://www.bleepingcomputer.com/news/security/malware-now-trying-to-exploit-new-windows-installer-zero-day/)