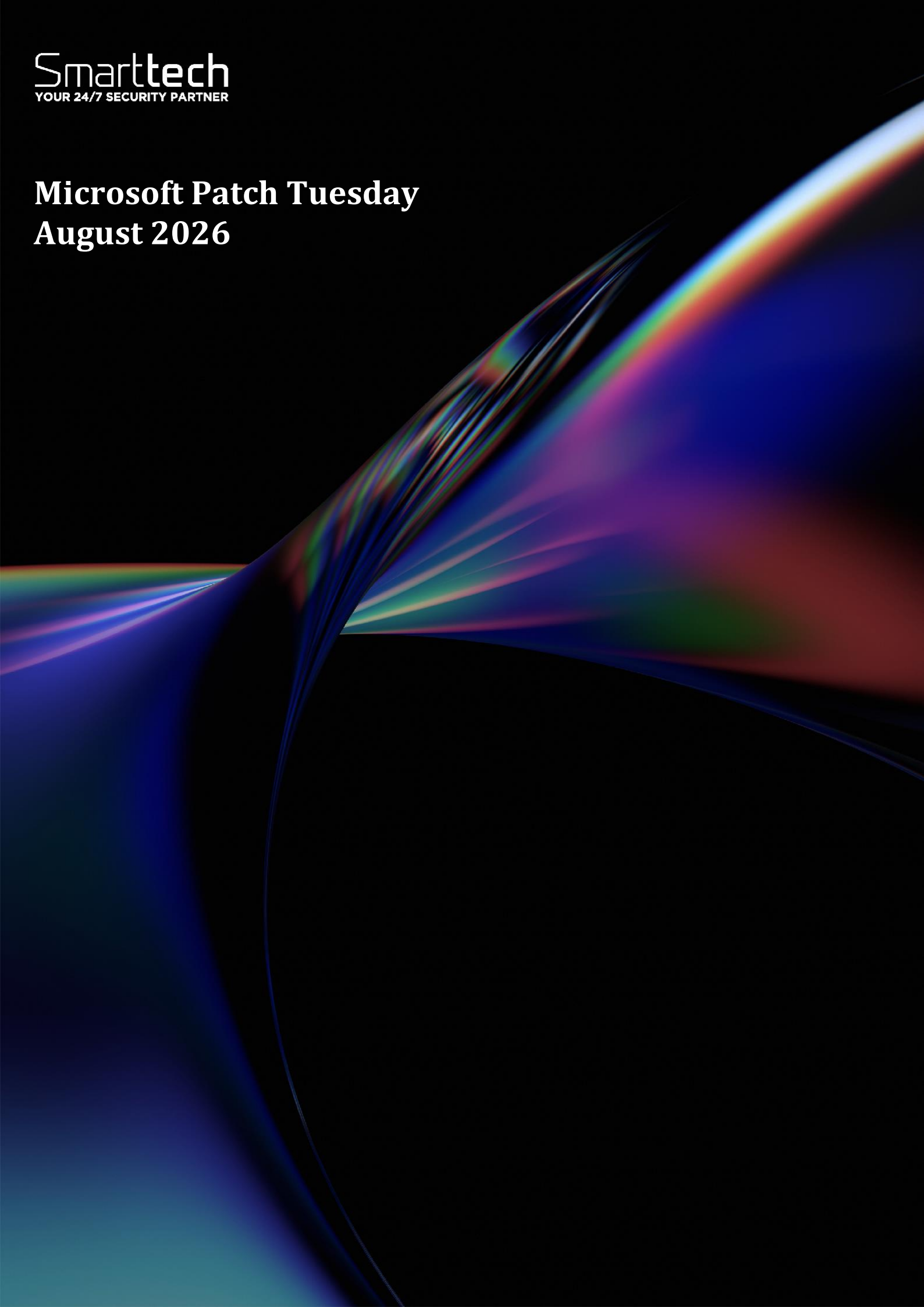
Smarttech
YOUR 24/7 SECURITY PARTNER

Microsoft Patch Tuesday
August 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	133
Authors	Mihaela-Liliana Matei < mihaela.matei@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-08-12
Issue Date	2026-08-12

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Microsoft patched 398 CVEs in its August 2026 Patch Tuesday release, with 42 rated Critical, 355 rated Important, and one rated as Moderate. The release includes three zero-days vulnerabilities, including one actively exploited and two publicly disclosed zero-day vulnerabilities. This Patch Tuesday addresses 42 Critical vulnerabilities, 37 of which are remote code execution and 5 are elevation of privilege. Elevation of Privilege vulnerabilities accounted for 40.7% of the vulnerabilities patched this month, followed by Remote Code Execution vulnerabilities at 27.1%.

CVE-2026-68820 is an EoP vulnerability affecting Windows Ancillary Function Driver for WinSock. It received a CVSSv3 score of 7.0 and was rated as important. A local attacker could exploit this vulnerability to elevate to SYSTEM privileges. According to Microsoft, this vulnerability was exploited in the wild as a zero-day.Two additional EoP vulnerabilities affecting this driver were patched this month. CVE-2026-61348 and CVE-2026-70307 also received CVSSv3 scores of 7.0, however no exploitation has been reported for these flaws. Both were assessed as "Exploitation More Likely" according to Microsoft's Exploitability Index.

CVE-2026-62832 is an elevation of privilege vulnerability affecting Windows User Profile Service. It received a CVSSv3 score of 7.8 and is rated as important. A local attacker could exploit this vulnerability to gain ADMINISTRATOR privileges. It was publicly disclosed prior to a patch being available and was assessed as “Exploitation More Likely.”

CVE-2026-72971 is a tampering vulnerability affecting the Windows Container Isolation FS Filter Driver (unionfs.sys). It received a CVSSv3 score of 5.5 and is rated as important. It was publicly disclosed prior to a patch being available. Successful exploitation would allow a local attacker to perform tampering. Despite being publicly disclosed, Microsoft assesses this vulnerability as “Exploitation Unlikely.”

Risk

Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Medium

Systems Affected:

- .NET
- .NET Core
- .NET Framework
- AMD Zen
- Active Directory Certificate Services (AD CS)
- Application Information Services
- Azure Active Directory
- Azure CycleCloud
- Azure Monitor Agent
- Azure Storage Explorer
- Capability Access Management Service (camsvc)
- Desktop Window Manager
- Dynamics Business Central
- GitHub Copilot and Visual Studio Code
- Microsoft Azure Attestation service and Device Health Attestation Service
- Microsoft COM for Windows
- Microsoft Defender for Endpoint
- Microsoft Digest Authentication
- Microsoft Dynamics 365 (on-premises)
- Microsoft Entra Connect Sync
- Microsoft Exchange Server
- Microsoft High Performance Computing (HPC) Pack
- Microsoft Identity Services
- Microsoft Local Security Authority Server (lsasrv)
- Microsoft Office
- Microsoft Office Access
- Microsoft Office Excel
- Microsoft Office Graphics Component
- Microsoft Office Outlook
- Microsoft Office PowerPoint
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft OneDrive
- Microsoft PowerShell

- Microsoft PowerShell Core
- Microsoft QUIC
- Microsoft Remote Registry Service
- Microsoft Teams Mobile
- Microsoft Teams for Android
- Microsoft Windows Codecs Library
- Microsoft Windows Media Foundation
- Microsoft Windows Search Component
- Power BI
- RPC Runtime
- Reliable Multicast Transport Driver (RMCAST)
- Remote Desktop Client
- User-Mode Power Service (UMPS)
- Virtual Hard Disk (VHD) Miniport Driver
- Visual Studio Code
- Visual Studio Code - Python extension
- Visual Studio Code CoPilot Chat Extension
- Windows Accessibility Infrastructure (ATBroker.exe)
- Windows Active Directory
- Windows Ancillary Function Driver for WinSock
- Windows Autopilot
- Windows Backup Engine
- Windows Bind Filter Driver
- Windows Cloud Files Mini Filter Driver
- Windows Common Log File System Driver
- Windows Container Isolation FS Filter Driver (unionfs.sys)
- Windows Cross Device Service
- Windows DHCP Client
- Windows DHCP Server
- Windows DNS
- Windows DWM Core Library
- Windows Defender Firewall Service
- Windows Deployment Services
- Windows Device Association Service
- Windows Display Enhancement Service
- Windows Encrypting File System (EFS)
- Windows Event Logging Service
- Windows GDI
- Windows GDI+
- Windows Graphics Kernel
- Windows HTTP Protocol Stack
- Windows HTTP.sys
- Windows Hello
- Windows Hyper-V
- Windows Imaging Component

- Windows Installer
- Windows Kerberos
- Windows Kernel
- Windows Key Guard
- Windows LDAP - Lightweight Directory Access Protocol
- Windows LUAFV
- Windows License Manager
- Windows MIDI Service Module
- Windows Management Instrumentation
- Windows Management Services
- Windows Message Queuing
- Windows Modern Device Management (MDM)
- Windows NTFS
- Windows Narrator Braille
- Windows Network Address Translation (NAT)
- Windows Network Connection Broker
- Windows Network File System
- Windows Package Manager
- Windows Program Compatibility Assistant Service
- Windows Projected File System
- Windows Push Notifications
- Windows RPC API
- Windows Remote Access API
- Windows Remote Access Connection Manager
- Windows Remote Desktop Services
- Windows Remote Help
- Windows Remote Help Defense
- Windows Routing and Remote Access Service (RRAS)
- Windows SMB Client
- Windows SMB Server
- Windows Schannel
- Windows Secure Socket Tunneling Protocol (SSTP)
- Windows Sensor Data Service
- Windows Shell
- Windows Storage
- Windows Storage Port Driver
- Windows TCP/IP
- Windows Telephony Service
- Windows USB Driver
- Windows Universal Disk Format File System Driver (UDFS)
- Windows User Profile Service
- Windows Win32K
- Windows Wired AutoConfig Service
- Windows Work Folder Service
- Windows iSCSI Target Service

- Winlogon

Technology	Products Affected	Severity	Reference	Workaround/ Exploited / Publicly Disclosed	Vulnerability Info
Windows	Windows 10, 11 Server 2012, 2012 R2, 2016, 2019, 2022, 2025 including Server Core Installations Remote Desktop Web Client Windows App Client for Windows Desktop Windows Admin Cente	Critical	CVE-2026-42976 CVE-2026-49179 CVE-2026-50472 CVE-2026-54113 CVE-2026-54984 CVE-2026-56171 CVE-2026-56174 CVE-2026-56179 CVE-2026-58598 CVE-2026-58643 CVE-2026-59122 CVE-2026-59124 CVE-2026-59125 CVE-2026-59126 CVE-2026-59127 CVE-2026-59128 CVE-2026-59130 CVE-2026-59131 CVE-2026-59132 CVE-2026-59133 CVE-2026-59134 CVE-2026-59135 CVE-2026-59136	Workaround: No ***Exploited: Yes***** ***Public: Yes****	Denial of Service Elevation of Privilege Information Disclosure Remote Code Execution Security Feature Bypass Spoofing Tampering

			CVE-2026-59137 CVE-2026-59138 CVE-2026-61345 CVE-2026-61346 CVE-2026-61347 CVE-2026-61348 CVE-2026-61349 CVE-2026-61350 CVE-2026-61352 CVE-2026-61353 CVE-2026-61355 CVE-2026-61356 CVE-2026-61357 CVE-2026-61358 CVE-2026-61359 CVE-2026-61360 CVE-2026-61361 CVE-2026-61363 CVE-2026-61364 CVE-2026-61365 CVE-2026-61366 CVE-2026-61367 CVE-2026-61368 CVE-2026-61918 CVE-2026-61920 CVE-2026-61921 CVE-2026-61923 CVE-2026-		

			61924 CVE-2026-61925 CVE-2026-61926 CVE-2026-61927 CVE-2026-61928 CVE-2026-61929 CVE-2026-61930 CVE-2026-61932 CVE-2026-61933 CVE-2026-61934 CVE-2026-61936 CVE-2026-61937 CVE-2026-61938 CVE-2026-61939 CVE-2026-62688 CVE-2026-62690 CVE-2026-62692 CVE-2026-62693 CVE-2026-62695 CVE-2026-62696 CVE-2026-62698 CVE-2026-62699 CVE-2026-62700 CVE-2026-62701 CVE-2026-62702 CVE-2026-62703 CVE-2026-62705 CVE-2026-62707		

			CVE-2026-62708 CVE-2026-62709 CVE-2026-62710 CVE-2026-62711 CVE-2026-62712 CVE-2026-62713 CVE-2026-62714 CVE-2026-62715 CVE-2026-62716 CVE-2026-62717 CVE-2026-62718 CVE-2026-62719 CVE-2026-62720 CVE-2026-62721 CVE-2026-62722 CVE-2026-62723 CVE-2026-62724 CVE-2026-62725 CVE-2026-62726 CVE-2026-62728 CVE-2026-62729 CVE-2026-62730 CVE-2026-62732 CVE-2026-62733 CVE-2026-62734 CVE-2026-62735 CVE-2026-62736 CVE-2026-		

			CVE-2026-62737 CVE-2026-62738 CVE-2026-62739 CVE-2026-62740 CVE-2026-62741 CVE-2026-62742 CVE-2026-62743 CVE-2026-62745 CVE-2026-62746 CVE-2026-62747 CVE-2026-62748 CVE-2026-62749 CVE-2026-62750 CVE-2026-62751 CVE-2026-62752 CVE-2026-62753 CVE-2026-62754 CVE-2026-62755 CVE-2026-62757 CVE-2026-62758 CVE-2026-62761 CVE-2026-62766 CVE-2026-62768 CVE-2026-62769 CVE-2026-62770 CVE-2026-62771 CVE-2026-62772 CVE-2026-62773		

			CVE-2026-62774 CVE-2026-62775 CVE-2026-62776 CVE-2026-62777 CVE-2026-62778 CVE-2026-62779 CVE-2026-62780 CVE-2026-62781 CVE-2026-62782 CVE-2026-62783 CVE-2026-62784 CVE-2026-62785 CVE-2026-62786 CVE-2026-62787 CVE-2026-62788 CVE-2026-62790 CVE-2026-62792 CVE-2026-62793 CVE-2026-62795 CVE-2026-62796 CVE-2026-62797 CVE-2026-62798 CVE-2026-62799 CVE-2026-62800 CVE-2026-62803 CVE-2026-62807 CVE-2026-62811 CVE-2026-		

			62812 CVE-2026-62814 CVE-2026-62815 CVE-2026-62816 CVE-2026-62817 CVE-2026-62818 CVE-2026-62819 CVE-2026-62820 CVE-2026-62822 CVE-2026-62823 CVE-2026-62824 ***CVE-2026-62832**** CVE-2026-62876 CVE-2026-62877 CVE-2026-62878 CVE-2026-62880 CVE-2026-62881 CVE-2026-62883 CVE-2026-62885 CVE-2026-62887 CVE-2026-62888 CVE-2026-62889 CVE-2026-62890 CVE-2026-62892 CVE-2026-62893 CVE-2026-62894 CVE-2026-62908 CVE-2026-65662		

			CVE-2026-65671 CVE-2026-65672 CVE-2026-65678 CVE-2026-65679 CVE-2026-65681 CVE-2026-65773 CVE-2026-65774 CVE-2026-65775 CVE-2026-65776 CVE-2026-65777 CVE-2026-65778 CVE-2026-65779 CVE-2026-65780 CVE-2026-65781 CVE-2026-65782 CVE-2026-65783 CVE-2026-65784 CVE-2026-65785 CVE-2026-65786 CVE-2026-65787 CVE-2026-65788 CVE-2026-65789 CVE-2026-65790 CVE-2026-65791 CVE-2026-65794 CVE-2026-65795 CVE-2026-65796 CVE-2026-		

			65797 CVE-2026-65798 CVE-2026-65799 CVE-2026-65814 CVE-2026-66799 CVE-2026-66802 CVE-2026-66804 CVE-2026-68819 ***CVE-2026-68820**** CVE-2026-70304 CVE-2026-70307 CVE-2026-70330 CVE-2026-70344 CVE-2026-70345 CVE-2026-70346 CVE-2026-70347 CVE-2026-70348 CVE-2026-71331 ***CVE-2026-72971****		
Exchange	Server 2016 CU23 Server 2019 CU14, CU15 Server Subscription Edition RTM Exchange Online	Critical	CVE-2026-56191 CVE-2026-62910 CVE-2026-62911 CVE-2026-62912 CVE-2026-62913 CVE-2026-62914 CVE-2026-62915 CVE-2026-65813	Workaround: No Exploited: No Public: No	Denial of Service Elevation of Privilege Remote Code Execution Security Feature Bypass Spoofing Tampering

SQL Server	Power BI Report Server	Important	CVE-2026-65811	Workaround: No Exploited: No Public: No	Remote Code Execution
Edge	Edge (Chromium-based) Edge for Android Surface Management Services	Critical	CVE-2026-54120 CVE-2026-57978 CVE-2026-57980 CVE-2026-57989 CVE-2026-57990 CVE-2026-62828 CVE-2026-65802 CVE-2026-65804 CVE-2026-66310 CVE-2026-66311 CVE-2026-66312 CVE-2026-66313 CVE-2026-66314 CVE-2026-66315 CVE-2026-66316 CVE-2026-66317 CVE-2026-66318 CVE-2026-66321 CVE-2026-66322 CVE-2026-66325 CVE-2026-66326 CVE-2026-70339	Workaround: No Exploited: No Public: No	Information Disclosure Remote Code Execution Spoofing Tampering
Office	365 Apps for Enterprise Access/Excel/Word/Outlook/ PowerPoint 2016	Critical	CVE-2026-58651 CVE-2026-62842 CVE-2026-	Workaround: No Exploited: No Public: No	Elevation of Privilege Information

	Office 2016, 2019 LTSC 2021, 2024 including for Mac Office 365 for Mac Teams (including for Android and iOS) OneDrive for MacOS		62870 CVE-2026-62882 CVE-2026-62896 CVE-2026-62918 CVE-2026-63513 CVE-2026-63515 CVE-2026-63517 CVE-2026-63518 CVE-2026-63519 CVE-2026-63521 CVE-2026-63524 CVE-2026-63525 CVE-2026-63526 CVE-2026-63527 CVE-2026-63528 CVE-2026-63529 CVE-2026-63530 CVE-2026-63531 CVE-2026-63532 CVE-2026-63533 CVE-2026-64898 CVE-2026-64899 CVE-2026-64903 CVE-2026-64904 CVE-2026-64905 CVE-2026-64906 CVE-2026-64907 CVE-2026-64908		Disclosure Remote Code Execution Spoofing

			CVE-2026-64909 CVE-2026-64910 CVE-2026-64911 CVE-2026-64912 CVE-2026-64914 CVE-2026-64915 CVE-2026-64917 CVE-2026-64919 CVE-2026-64920 CVE-2026-65656 CVE-2026-65657 CVE-2026-65661 CVE-2026-65664 CVE-2026-65667 CVE-2026-65680 CVE-2026-65767 CVE-2026-65768 CVE-2026-65769 CVE-2026-65807 CVE-2026-66806 CVE-2026-66807 CVE-2026-66809 CVE-2026-66810 CVE-2026-68792 CVE-2026-68793 CVE-2026-68794 CVE-2026-68795 CVE-2026-		

			68796 CVE-2026-68797 CVE-2026-68798 CVE-2026-68799 CVE-2026-68800 CVE-2026-68801 CVE-2026-68802 CVE-2026-68803 CVE-2026-68804 CVE-2026-68805 CVE-2026-68806 CVE-2026-68807 CVE-2026-68808 CVE-2026-68809 CVE-2026-68810 CVE-2026-68811 CVE-2026-68812 CVE-2026-68813 CVE-2026-68814 CVE-2026-68815 CVE-2026-68816 CVE-2026-68817 CVE-2026-70130 CVE-2026-70310 CVE-2026-70311 CVE-2026-70312 CVE-2026-70313 CVE-2026-70314		

			CVE-2026-70315 CVE-2026-70316 CVE-2026-70317 CVE-2026-70318 CVE-2026-70319 CVE-2026-70320 CVE-2026-70322 CVE-2026-70323 CVE-2026-70325 CVE-2026-70327 CVE-2026-70328 CVE-2026-70329		
SharePoint	Enterprise Server 2016 Server 2019 Server Subscription Edition SharePoint Online	Critical	CVE-2026-57105 CVE-2026-58639 CVE-2026-62826 CVE-2026-62827 CVE-2026-62829 CVE-2026-62837 CVE-2026-62839 CVE-2026-62917 CVE-2026-63512 CVE-2026-63514 CVE-2026-63516 CVE-2026-63520 CVE-2026-64897 CVE-2026-64900 CVE-2026-64901	Workaround: No Exploited: No Public: No	Elevation of Privilege Information Disclosure Remote Code Execution Spoofing Tampering

			CVE-2026-64902 CVE-2026-64916 CVE-2026-64921 CVE-2026-64922 CVE-2026-65658 CVE-2026-65660 CVE-2026-65663 CVE-2026-65665 CVE-2026-66805 CVE-2026-66808 CVE-2026-70306 CVE-2026-70321 CVE-2026-70324 CVE-2026-70326 CVE-2026-70332 CVE-2026-70355		
Azure	Application Insights Profiler Azure Active Directory AI Service API Management (APIM) App Service for Linux Confidential Ledger Cosmos DB CycleCloud 8.9.1/8.9.2 DNS Key Vault	Critical	CVE-2026-35425 CVE-2026-47299 CVE-2026-49159 CVE-2026-49163 CVE-2026-50481 CVE-2026-50515 CVE-2026-50516 CVE-2026-56160 CVE-2026-56161 CVE-2026-56162 CVE-2026-56163	Workaround: No Exploited: No Public: No	Elevation of Privilege Information Disclosure Remote Code Execution Spoofing

	Kubernetes Service Logic Apps Monitor Agent Linux Extension Portal Red Hat OpenShift (ARO) Service Bus SQL Database SQL Managed Instance SRE Agent 365 Admin Center Microsoft Account MS Entra Connect MS Entra ID MS Entra Provisioning Service MS Graph MS Purview Data Governance MS Purview eDiscovery		CVE-2026-56165 CVE-2026-56167 CVE-2026-57106 CVE-2026-58275 CVE-2026-58630 CVE-2026-59115 CVE-2026-62825 CVE-2026-62830 CVE-2026-62835 CVE-2026-62836 CVE-2026-62869 CVE-2026-62873 CVE-2026-63522 CVE-2026-65668 CVE-2026-65673 CVE-2026-65806 CVE-2026-66803 CVE-2026-68823 CVE-2026-70340		
Developer Tools	.NET 8, 9, 10 installed on Linux, MacOS and Windows .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.8.1 Visual Studio 2022 17.14, 2026 18.8 Visual Studio Code Visual Studio Code CoPilot Chat Extension	Important	CVE-2026-47285 CVE-2026-54981 CVE-2026-58612 CVE-2026-58641 CVE-2026-58650 CVE-2026-59113 CVE-2026-59119 CVE-2026-62871	Workaround: No Exploited: No Public: No	Denial of Service Elevation of Privilege Information Disclosure Remote Code Execution Security Feature Bypass

	PowerShell 7.4, 7.5, 7.6 Python extension for Visual Studio Code		CVE-2026-62872 CVE-2026-62886 CVE-2026-62897 CVE-2026-62898 CVE-2026-62899 CVE-2026-62900 CVE-2026-62901 CVE-2026-62902 CVE-2026-62909 CVE-2026-65675 CVE-2026-65810 CVE-2026-69278 CVE-2026-69306 CVE-2026-69320 CVE-2026-70335 CVE-2026-70336 CVE-2026-70337 CVE-2026-70338 CVE-2026-70354		
Dynamics	CoPilot Cowork 365 (on-premises) v9.1 365 Business Central 2024 Release Wave 2, 2025 Release Wave 1 & 2, 2026 Release Wave 1	Critical	CVE-2026-40375 CVE-2026-59118 CVE-2026-65815 CVE-2026-66301	Workaround: No Exploited: No Public: No	Elevation of Privilege Information Disclosure Remote Code Execution
Device	MS Planetary Computer Pro (GeoCatalog)	Critical	CVE-2026-63508	Workaround: No Exploited: No Public: No	Elevation of Privilege

Apps	Installer 365 CoPilot Windows Terminal App	Critical	CVE-2026-50517 CVE-2026-59117 CVE-2026-68821	Workaround: No Exploited: No Public: No	Elevation of Privilege Remote Code Execution
System Center	Defender for EndPoint for Mac	Important	CVE-2026-54123	Workaround: No Exploited: No Public: No	Information Disclosure
Open Source Software	Azure Storage Explorer	Important	CVE-2026-57104	Workaround: No Exploited: No Public: No	Elevation of Privilege

Recommendations

Smarttech247 team recommend the following actions to be taken:

- Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

- Apply the Principle of Least Privilege to all systems and services, and run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- Remind all users not to visit untrusted websites or follow links/open files provided by unknown or untrusted sources. (**M1017: User Training**)

- **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
- **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
  - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
  - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response client or host-based IPS agent.

References

https://www.tenable.com/blog/microsofts-august-2026-patch-tuesday-addresses-398-cves-cve-2026-68820

https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2026-patch-tuesday-fixes-400-flaws-3-zero-days/


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com