Smarttech
YOUR 24/7 SECURITY PARTNER

Microsoft Patch Tuesday
September 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	154
Authors	Denis Bojian <denis.bojian@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-09
Issue Date	2026-09-09

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's September 2026 Patch Tuesday is its largest release on record(the total at 964 CVEs (104 Critical, 860 Important), while BleepingComputer — which counts only flaws issued on Patch Tuesday itself — puts it at 966 CVEs, including 105 rated Critical (81 remote code execution, 20 elevations of privilege, 2 information disclosure, 1 security feature bypass). Both figures surpass the previous record set in July 2026. The release includes two zero-day vulnerabilities that were actively exploited in the wild prior to patching, both rated "Important" rather than Critical. Elevation of Privilege vulnerabilities accounted for the largest share of this month's updates (44.7%), followed by Remote Code Execution vulnerabilities (26.8%).

Zero-days patched this month (both actively exploited, both rated Important):

CVE-2026-81963 — Windows Update Stack Elevation of Privilege Vulnerability (CVSS 7.8). A link-following flaw allows an authenticated attacker to gain SYSTEM privileges. Credited to Romain Deperne and Microsoft's MSTIC team.

CVE-2026-85880 — Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability (CVSS 7.8). A heap-based buffer overflow allows SYSTEM-level privilege elevation. Discovered by Volexity and researchers at Proofpoint.

Risk

Government:
- Large and medium-sized 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 and Visual Studio
* ASP.NET Core
* Active Directory Certificate Services (AD CS)
* Active Directory Domain Services
* Active Directory Federation Services (AD FS)
* Audio Video Control Transport Protocol
* Azure Arc
* Azure CycleCloud
* Azure HDInsights
* BranchCache
* Connected Devices Platform Service (Cdpsvc)
* Data Sharing Service Client
* GitHub Copilot and Visual Studio Code
* Graphic Fonts
* HID class driver
* IP Helper
* Internet Storage Name Service
* Kernel Streaming WOW Thunk Service Driver
* Microsoft Account
* Microsoft Authenticator
* Microsoft Azure Attestation service and Device Health Attestation Service
* Microsoft Azure CLI
* Microsoft COM for Windows
* Microsoft Dynamics 365
* Microsoft Exchange Server
* Microsoft Graphics Component
* Microsoft Install Service
* Microsoft JScript
* Microsoft Local Security Authority Server (lsasrv)
* Microsoft Office (Access, Excel, Outlook, PowerPoint, Publisher, SharePoint, Word)
* Microsoft Standard XPS
* Microsoft Teams for Android
* Microsoft Trace Data Helper
* Microsoft UxTheme Library
* Microsoft WDAC OLE DB provider for SQL
* Microsoft WebP Image Extension
* Microsoft Windows Codecs Library
* Microsoft Windows Media Foundation
* Microsoft Windows PDF
* Microsoft Windows Search Component
* Microsoft Windows Speech
* OpenSSH for Windows

* Power Automate
* RPC Runtime
* Reliable Multicast Transport Driver (RMCAST)
* Remote Desktop Client
* Remote Desktop Gateway Service
* Role: DNS Server
* Role: Windows Fax Service
* SQL Server
* Skype for Business
* Spring Cloud Azure
* Storage Port Driver
* Telnet Client
* Virtual Hard Disk (VHD) Miniport Driver
* Visual Studio / Visual Studio Code
* Volume Manager Driver
* Windows ALPC
* Windows Authentication Methods
* Windows Autopilot
* Windows BitLocker
* Windows Bluetooth Port Driver/Service
* Windows Boot Manager
* Windows Cloud Files Mini Filter Driver
* Windows Connected User Experiences and Telemetry
* Windows Credential Guard/Providers
* Windows DCOM Server
* Windows DHCP Client/Server
* Windows DNS
* Windows DWM Core Library
* Windows Defender Firewall Service
* Windows Distributed File System (DFS)
* Windows Encrypting File System (EFS)
* Windows Error Reporting
* Windows Event Logging Service
* Windows Failover Cluster
* Windows GDI/GDI+
* Windows Graphics Kernel
* Windows Group Policy
* Windows HTTP.sys
* Windows Hello
* Windows Hyper-V
* Windows IKE Extension
* Windows Kerberos
* Windows Kernel / Kernel Mode Driver
* Windows LDAP
* Windows Management Instrumentation

* Windows Media Player
* Windows Message Queuing
* Windows NTFS
* Windows Netlogon
* Windows Network File System
* Windows OLE DB
* Windows PowerShell
* Windows Print Spooler Components
* Windows RDP / Remote Desktop Services
* Windows Registry
* Windows Remote Desktop Licensing Service
* Windows Resilient File System (ReFS)
* Windows Routing and Remote Access Service (RRAS)
* Windows SMB Client/Server
* Windows Schannel
* Windows Secure Boot
* Windows Server
* Windows Shell
* Windows Storage
* Windows TCP/IP
* Windows Task Scheduler
* Windows USB drivers (Audio Class, Hub, Mass Storage, Video)
* Windows Update Stack
* Windows Win32K
* Windows Wireless Networking
* Xbox Gaming Services

Technology	Products Affected	Severity	Reference	Workaround/ Exploited / Publicly Disclosed	Vulnerability Info
Azure AI Language	Azure AI Language	Critical	CVE-2026-70352	Workaround: No Exploited: No Public: No	Elevation of Privilege
Azure Cosmos DB	Azure Cosmos DB	Critical	CVE-2026-69857	Workaround: No Exploited: No Public: No	Spoofing
Copilot Studio	Copilot Studio	Critical	CVE-2026-80098	Workaround: No Exploited: No Public: No	Elevation of Privilege

Entra ID	Entra ID	Critical	CVE-2026-83941 CVE-2026-62916	Workaround: No Exploited: No Public: No	Elevation of Privilege
Microsoft Azure Active Directory B2C	Microsoft Azure Active Directory B2C	Critical	CVE-2026-83711	Workaround: No Exploited: No Public: No	Elevation of Privilege
Microsoft Discovery Studio	Microsoft Discovery Studio	Critical	CVE-2026-62906	Workaround: No Exploited: No Public: No	Information Disclosure
Microsoft Dynamics 365	Microsoft Dynamics 365 On-Premises	Critical	CVE-2026-65772	Workaround: No Exploited: No Public: No	Remote Code Execution
Microsoft Fabric	Microsoft Fabric	Critical	CVE-2026-70178	Workaround: No Exploited: No Public: No	Elevation of Privilege
Microsoft Office	Microsoft Office Microsoft Office Word Microsoft Office Excel Microsoft Office PowerPoint Microsoft Office Outlook	Critical	CVE-2026-69285 CVE-2026-78505 CVE-2026-77898 CVE-2026-69632 CVE-2026-78510 CVE-2026-81952 CVE-2026-77504 CVE-2026-81949 CVE-2026-	Workaround: No Exploited: No Public: No	Remote Code Execution Information Disclosure

			81948 CVE-2026-81950 CVE-2026-81959 CVE-2026-81953 CVE-2026-81951 CVE-2026-69678 CVE-2026-69797 CVE-2026-69767 CVE-2026-78509 CVE-2026-78520 CVE-2026-78525 CVE-2026-78519		
Graphic Fonts	Graphic Fonts	Critical	CVE-2026-72986 CVE-2026-73018	Workaround: No Exploited: No Public: No	Remote Code Execution
IP Helper	IP Helper	Critical	CVE-2026-72981	Workaround: No Exploited: No Public: No	Remote Code Execution
Microsoft Graphics Component	Microsoft Graphics Component	Critical	CVE-2026-78439 CVE-2026-81955 CVE-2026-73006	Workaround: No Exploited: No Public: No	Remote Code Execution

			CVE-2026-77493		
Microsoft WebP Image Extension	Microsoft WebP Image Extension	Critical	CVE-2026-70351	Workaround: No Exploited: No Public: No	Remote Code Execution
Microsoft Windows Codecs Library	Microsoft Windows Codecs Library	Critical	CVE-2026-81352 CVE-2026-58599	Workaround: No Exploited: No Public: No	Remote Code Execution
Microsoft Windows Media Foundation	Microsoft Windows Media Foundation	Critical	CVE-2026-69601	Workaround: No Exploited: No Public: No	Remote Code Execution
Power Automate	Power Automate	Critical	CVE-2026-65818	Workaround: No Exploited: No Public: No	Elevation of Privilege
Reliable Multicast Transport Driver (RMCAST)	Reliable Multicast Transport Driver (RMCAST)	Critical	CVE-2026-78449 CVE-2026-78450 CVE-2026-69530	Workaround: No Exploited: No Public: No	Remote Code Execution
Role: DNS Server	Role: DNS Server	Critical	CVE-2026-69827 CVE-2026-77505	Workaround: No Exploited: No Public: No	Remote Code Execution
Skype for Business	Skype for Business	Critical	CVE-2026-66302	Workaround: No Exploited: No Public: No	Remote Code Execution
Spring Cloud Azure	Spring Cloud Azure	Critical	CVE-2026-69854	Workaround: No	Elevation of Privilege

				Exploited: No Public: No	
SQL Server	SQL Server	Critical	CVE-2026-67378 CVE-2026-67631 CVE-2026-65669 CVE-2026-67643 CVE-2026-67636	Workaround: No Exploited: No Public: No	Remote Code Execution Elevation of Privilege
Virtual Hard Disk (VHD) Miniport Driver	Virtual Hard Disk (VHD) Miniport Driver	Critical	CVE-2026-81355	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows ALPC	Windows Advanced Local Procedure Call (ALPC)	Critical Important	CVE-2026-69874 CVE-2026-85880	Workaround: No Exploited: CVE-2026-85880 is actively exploited Public: No	Elevation of Privilege
Windows Credential Guard	Windows Credential Guard	Critical	CVE-2026-72958	Workaround: No Exploited: No Public: No	Elevation of Privilege
Windows Deployment Services	Windows Deployment Services	Critical	CVE-2026-72954 CVE-2026-72957	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows DNS	Windows DNS	Critical	CVE-2026-69858 CVE-2026-69813 CVE-2026-	Workaround: No Exploited: No Public: No	Remote Code Execution

			69730 CVE-2026-72987		
Windows Failover Cluster	Windows Failover Cluster	Critical	CVE-2026-73010 CVE-2026-78444	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Graphics Kernel	Windows Graphics Kernel	Critical	CVE-2026-73017	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Hello	Windows Hello	Critical	CVE-2026-69784 CVE-2026-81354 CVE-2026-69740 CVE-2026-69799 CVE-2026-69820 CVE-2026-69864 CVE-2026-69710 CVE-2026-69725 CVE-2026-72980	Workaround: No Exploited: No Public: No	Elevation of Privilege Security Feature Bypass
Windows HTTP Print Provider	Windows HTTP Print Provider	Critical	CVE-2026-69769	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Hyper-V	Windows Hyper-V	Critical	CVE-2026-72961 CVE-2026-69603	Workaround: No Exploited: No	Elevation of Privilege Remote Code

			CVE-2026-80083	Public: No	Execution
Windows Imaging Component	Windows Imaging Component	Critical	CVE-2026-73023 CVE-2026-77495 CVE-2026-73013 CVE-2026-70296 CVE-2026-69860 CVE-2026-69499	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Internet Connection Sharing (ICS)	Windows Internet Connection Sharing (ICS)	Critical	CVE-2026-72983	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Kerberos	Windows Kerberos	Critical	CVE-2026-69676	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Key Distribution Center	Windows Key Distribution Center	Critical	CVE-2026-69712	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Media Player	Windows Media Player	Critical	CVE-2026-70203 CVE-2026-72960	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Message Queuing	Windows Message Queuing	Critical	CVE-2026-69579	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows	Windows Netlogon	Critical	CVE-2026-72982	Workaround:	Remote Code

Netlogon				No Exploited: No Public: No	Execution
Windows Paint	Windows Paint	Critical	CVE-2026-70586	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Raw Image Extension	Windows Raw Image Extension	Critical	CVE-2026-69649	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Remote Desktop	Windows Remote Desktop	Critical	CVE-2026-69518	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Routing and Remote Access Service (RRAS)	Windows Routing and Remote Access Service (RRAS)	Critical	CVE-2026-72959 CVE-2026-69590 CVE-2026-69852 CVE-2026-72950	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Secure Kernel Mode	Windows Secure Kernel Mode	Critical	CVE-2026-69501 CVE-2026-83939 CVE-2026-69846 CVE-2026-69906	Workaround: No Exploited: No Public: No	Elevation of Privilege
Windows Secure Socket Tunneling Protocol (SSTP)	Windows Secure Socket Tunneling Protocol (SSTP)	Critical	CVE-2026-73009	Workaround: No Exploited: No Public: No	Remote Code Execution

Windows Services for NFS ONCRPC XDR Driver	Windows Services for NFS ONCRPC XDR Driver	Critical	CVE-2026-69595 CVE-2026-70585 CVE-2026-78445	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows Shell	Windows Shell	Critical	CVE-2026-69829	Workaround: No Exploited: No Public: No	Remote Code Execution
Windows USB Video Driver	Windows USB Video Driver	Critical	CVE-2026-72962	Workaround: No Exploited: No Public: No	Elevation of Privilege
Windows Virtual Trusted Platform Module	Windows Virtual Trusted Platform Module	Critical	CVE-2026-69890	Workaround: No Exploited: No Public: No	Elevation of Privilege
Windows Virtualization-Based Security (VBS) Enclave	Windows Virtualization-Based Security (VBS) Enclave	Critical	CVE-2026-83501 CVE-2026-83498	Workaround: No Exploited: No Public: No	Information Disclosure Elevation of Privilege
Mariner	Mariner	Critical	CVE-2026-85506 CVE-2026-85507 CVE-2026-85508 CVE-2026-85509 CVE-2026-85504	Workaround: No Exploited: No Public: No	Buffer Overflow
Windows Update Stack	Windows Update Stack	Important	CVE-2026-81963	Workaround: No Exploited: Yes	Elevation of Privilege

				Public: No	

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

September 2026 Microsoft Patch Tuesday | Tenable®

https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2026-patch-tuesday-fixes-966-flaws-2-zero-days/

https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/Microsoft-Patch-Tuesday-September-2026.html

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com