Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's September 2026 Patch Tuesday - Priority Fixes

Date of Publication	Admiralty Code	TA Number
September 09, 2026	A1	TA2026264

Summary

First Seen: September 8, 2026
Affected Platforms: Microsoft Windows Advanced Local Procedure Call (ALPC), Microsoft Windows Update Stack, Microsoft Windows Deployment Services, Microsoft Windows NTFS, Microsoft Windows DHCP Client, Microsoft Windows DNS Server, Microsoft Windows Remote Desktop Services, Microsoft Windows Services for NFS ONCRPC XDR Driver, Microsoft Windows Routing and Remote Access Service (RRAS), Microsoft Windows Kerberos, Microsoft Azure Cosmos DB, Spring Cloud Azure, Microsoft Malware Protection Engine (Microsoft Defender)
Impact: Information Disclosure, Denial of Service, Remote Code Execution, Elevation of Privilege, Security Feature Bypass, Spoofing, Tampering

Exploitable CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-85880	Microsoft Windows Heap-Based Buffer Overflow Vulnerability	Windows 10 Version 1809; Windows Server 2019, 2022, 2016, 2012; Windows 10 Version 21H2	✓	✓	✓
CVE-2026-81963	Microsoft Windows Link Following Vulnerability	Windows 11 Version 23H2, 24H2, 25H2; Windows Server 2025	✓	✓	✓
CVE-2026-72957	Windows Deployment Services Remote Code Execution Vulnerability	Windows 10 Version 1607, 1809; Windows Server 2012, 2016, 2025, 2022, 2019	✗	✗	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-71329	Windows NTFS Remote Code Execution Vulnerability	Windows 11 Version 25H2, 22H2, 26H1, 24H2, 23H2; Windows Server 2012, 2016, 2025, 2022, 2019; Windows 10 Version 1607, 1809	✗	✗	✓
CVE-2026-69777	Windows DHCP Client Elevation of Privilege Vulnerability	Windows 11 Version 26H1, 24H2, 25H2	✗	✗	✓
CVE-2026-69730	Windows DNS Server Remote Code Execution Vulnerability	Windows Server 2025, 2012, 2016; Windows 10 Version 1607	✗	✗	✓
CVE-2026-69525	Remote Desktop Services Remote Code Execution Vulnerability	Windows 11 Version 23H2, 24H2, 25H2, 26H1; Windows 10 Version 22H2; Windows Server 2012, 2016, 2025; Windows 10 Version 1607, 1809	✗	✗	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-68833	Windows NTFS Remote Code Execution Vulnerability	Windows Server 2012, 2016, 2025, 2022, 2019; Windows 10 Version 1607; Windows 11 Version 26H1, 24H2, 23H2, 25H2	✗	✗	✓
CVE-2026-83501	Windows Virtualization-Based Security (VBS) Information Disclosure Vulnerability	Windows 11 Version 26H1, 24H2, 23H2, 25H2; Windows Server 2025	✗	✗	✓
CVE-2026-70585	Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability	Windows Server 2019, 2022, 2025, 2016, 2012	✗	✗	✓
CVE-2026-69857	Azure Cosmos DB Spoofing Vulnerability	Azure Cosmos DB	✗	✗	✓
CVE-2026-69854	Spring Cloud Azure Elevation of Privilege Vulnerability	Spring Cloud Azure	✗	✗	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-69852	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Server 2012, 2016, 2025, 2022, 2019; Windows 10 Version 1607, 1809, 22H2, 21H2; Windows 11 Version 26H1, 24H2, 23H2, 25H2	✗	✗	✓
CVE-2026-69676	Windows Kerberos Remote Code Execution Vulnerability	Windows 10 Version 1607, 1809, 22H2, 21H2; Windows Server 2012, 2016, 2025; Windows 11 Version 26H1, 24H2, 23H2, 25H2; Windows Server 2022, 2019	✗	✗	✓
CVE-2026-69414	ShieldBreak (Microsoft Defender Elevation of Privilege Vulnerability)	Microsoft Malware Protection Engine	✗	✗	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	
Defense Evasion	T1574: Hijack Execution Flow	
	T1211: Exploitation for Defense Evasion	
Lateral Movement	T1210: Exploitation of Remote Services	
Collection	T1005: Data from Local System	
Credential Access	T1556: Modify Authentication Process	

Vulnerability Details

#1

Microsoft's September 2026 Patch Tuesday delivers an extensive batch of security updates, addressing 974 vulnerabilities across its product ecosystem. These include 113 rated critical and 861 marked important in severity. The vulnerabilities span various categories: 439 elevation-of-privilege flaws, 258 remote code execution issues, 173 information disclosure bugs, 56 denial-of-service vulnerabilities, 16 spoofing issues, 19 security feature bypasses, and 13 tampering issues. Beyond its own products, Microsoft also released patches for 23 non-Microsoft CVEs, pushing the total count of vulnerabilities addressed this month to 997. Notably, 15 of these CVEs are considered at risk of active exploitation, underscoring the urgency of prompt patch deployment.

#2

Among the standout flaws, two of the flaws were under active exploitation in the wild at the time of patching, and both have since been added to the CISA Known Exploited Vulnerabilities catalog with a federal remediation deadline of September 22, 2026. CVE-2026-85880 is a heap-based buffer overflow in Windows Advanced Local Procedure Call that permits an authorized local attacker to escape a low-privilege AppContainer sandbox and elevate to SYSTEM with no additional user interaction. CVE-2026-81963 is an improper link resolution flaw in the Windows Update Stack that allows a local attacker to cause the update mechanism to follow a malicious link and overwrite a legitimate system component with an attacker-controlled substitute, again yielding SYSTEM.

#3

Alongside the two zero-days, this advisory tracks a set of network-reachable critical remote code execution flaws in core Windows server roles, including Windows DNS Server (CVE-2026-69730), Windows Remote Desktop Services (CVE-2026-69525), Windows Routing and Remote Access Service (CVE-2026-69852), Windows Kerberos (CVE-2026-69676), Windows Deployment Services (CVE-2026-72957), and the Windows Services for NFS ONCRPC XDR Driver (CVE-2026-70585).

#4

Several of these are exploitable by an unauthenticated attacker over the network, placing internet-exposed and flat internal networks at direct risk of pre-authentication compromise of infrastructure services. The set also includes remote code execution in Windows NTFS (CVE-2026-71329 and CVE-2026-68833), local privilege escalation in the Windows DHCP Client (CVE-2026-69777), a spoofing flaw in Azure Cosmos DB (CVE-2026-69857), and an elevation of privilege flaw in Spring Cloud Azure (CVE-2026-69854).

#5

CVE-2026-69414 warrants separate treatment because its remediation status is contested. Publicly tracked as ShieldBreak, the flaw affects Microsoft Defender and was reported in August 2026. Microsoft addressed it in Microsoft Malware Protection Engine version 1.1.26080.3, delivered through the automatic definition and engine update channel, requiring no customer action. On September 9, 2026, a proof-of-concept named **ShieldCrash** asserted that Microsoft failed to properly patch ShieldBreak, stating that although several changes were made to prevent re-exploitation, one path was missed and the original condition can still be triggered under specific circumstances. The published proof-of-concept demonstrates arbitrary file read in the SYSTEM context on a host running the latest version of Windows, and all supported versions of the desktop operating system are reported to be impacted. Because the bypass is public and no vendor fix for it has been announced, the effective risk for this component should be treated as live rather than remediated.

Recommendations

- Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential patches or adopting security measures.
- Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.
- Prioritize patching the actively exploited vulnerabilities CVE-2026-85880 and CVE-2026-81963. These vulnerabilities pose significant exploitation risks and should be addressed urgently.
- Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.
- Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

References

https://msrc.microsoft.com/update-guide/releaseNote/2026-Sep

https://msrc.microsoft.com/update-guide/vulnerability

https://github.com/MSNightmare/ShieldCrash

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 9, 2026 • 7:00 PM

More at www.hivepro.com