Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft September 2025 Patch Tuesday Roundup

Date of Publication	Admiralty Code	TA Number
September 11, 2025	A1	TA2025278

Summary

First Seen: September 9, 2025
Affected Platforms: Microsoft SQL Server, Windows Graphics, Windows Update Service, Microsoft Office, Microsoft SharePoint, Google Chromium, and more
Impact: Information Disclosure, Denial of Service, Remote Code Execution, Elevation of Privilege, Security Feature Bypass, Spoofing

Exploitable CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-55234	Windows SMB Elevation of Privilege Vulnerability	Windows Server: 2025, 2022, 2019, 2012 R2, 2016; Windows 10 Version 21H2; Windows 11 Version: 21H2, 24H2	✗	✗	✓
CVE-2024-21907	Newtonsoft.Json Denial of Service Vulnerability	Microsoft SQL Server 2019, 2017, 2016	✗	✗	✓
CVE-2025-54918	Windows NTLM Elevation of Privilege Vulnerability	Windows Server 2012, 2008	✗	✗	✓
CVE-2025-54910	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office 2016, 2019; Microsoft Office LTSC for Mac 2024, 2021; Microsoft 365 Apps for Enterprise	✗	✗	✓
CVE-2025-53803	Windows Kernel Memory Information Disclosure Vulnerability	Windows Server 2025, 2022, 2012, 2016; Windows 10, 22H2; Windows 11 Version 24H2	✗	✗	✓
CVE-2025-53804	Windows Kernel-Mode Driver Information Disclosure Vulnerability	Windows Server 2025, 2022, 23H2, 2019, 2012, 2016; Windows 11 Version 24H2, 23H2; Windows 10	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-54093	Windows TCP/IP Driver Elevation of Privilege Vulnerability	Windows Server 2012, 2008	✗	✗	✓
CVE-2025-54098	Windows Hyper-V Elevation of Privilege Vulnerability	Windows Server 2025, 2022, 23H2, 2012, 2008, 2016; Windows 11 Version 24H2, 23H2; Windows 10	✗	✗	✓
CVE-2025-54110	Windows Kernel Elevation of Privilege Vulnerability	Windows Server 2025, 2022, 23H2, 2019, 2016, 2012, 2008; Windows 11 Version 24H2, 23H2; Windows 10, 22H2	✗	✗	✓
CVE-2025-54916	Windows NTFS Remote Code Execution Vulnerability	Windows Server 2012, 2008	✗	✗	✓
CVE-2025-53800	Windows Graphics Component Elevation of Privilege Vulnerability	Windows Server 2025, 2022, 23H2, 2019, 2016; Windows 11 Version 24H2, 23H2; Windows 10	✗	✗	✓
CVE-2025-55228	Windows Graphics Component Remote Code Execution Vulnerability	Windows Server 2025 2022, 23H2; Windows 11 Version 24H2; Windows 10 Version 22H2	✗	✗	✓
CVE-2025-9864	Google Chrome Use after free in V8 Vulnerability	Microsoft Edge (Chromium-based)	✗	✗	✓
CVE-2025-9866	Google Chrome Content Security Policy Bypass Vulnerability	Microsoft Edge (Chromium-based)	✗	✗	✓

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

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	TA0040 Impact
T1204 User Execution	T1189 Drive-by Compromise	T1021 Remote Services	T1566 Phishing
T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1068 Exploitation for Privilege Escalation
T1588.006 Vulnerabilities	T1498 Network Denial of Service	T1190 Exploit Public-Facing Application	T1569.002 Service Execution
T1018 Remote System Discovery	T1021.002 SMB/Windows Admin Shares	T1071.001 Web Protocols	T1033 System Owner/User Discovery
T1505 Server Software Component	T1569 System Services	T1112 Modify Registry	T1005 Data from Local System
T1543 Create or Modify System Process	T1543.003 Windows Service	T1047 Windows Management Instrumentation	T1562.001 Disable or Modify Tools
T1133 External Remote Services	T1218 System Binary Proxy Execution	T1562 Impair Defenses	T1210 Exploitation of Remote Services
T1087 Account Discovery	T1046 Network Service Discovery	T1499 Endpoint Denial of Service	T1204.002 Malicious File

Vulnerability Details

#1

Microsoft's September 2025 Patch Tuesday delivers a significant security update, addressing a total of 81 vulnerabilities across its product ecosystem. Of these, 8 are classified as critical, 72 as important, and 1 as moderate in severity. The vulnerabilities span multiple categories: 38 elevation of privilege, 22 remote code execution (RCE), 14 information disclosure, 3 denial of service, 3 security feature bypass, and 1 spoofing issue. Additionally, Microsoft has released patches for 5 non-Microsoft CVEs, bringing the total to 86 vulnerabilities addressed this month. Importantly, 14 of these vulnerabilities are at risk of exploitation, emphasizing the need for immediate patch deployment.

#2

One of the most concerning issues is the publicly disclosed vulnerability in Windows SMB (CVE-2025-55234). This flaw allows unauthenticated remote attackers to perform relay attacks by exploiting improper authentication mechanisms in SMB Server configurations. Systems lacking hardening measures, such as SMB Server signing or Extended Protection for Authentication (EPA), are particularly vulnerable. Exploitation could lead to privilege escalation, enabling attackers to compromise the confidentiality, integrity, and availability of affected systems.

#3

Another critical vulnerability is in the Newtonsoft.Json library (CVE-2024-21907), which affects versions prior to 13.0.1 and is integrated into Microsoft SQL Server. This flaw enables unauthenticated, remote attackers to cause a denial-of-service condition by exploiting improper handling of exceptional states.

#4

Two additional vulnerabilities demand close attention. CVE-2025-54918, a privilege escalation flaw in Windows NTLM, could allow attackers to gain SYSTEM-level privileges. Meanwhile, CVE-2025-54910, a critical remote code execution vulnerability in Microsoft Office, permits unauthenticated local attackers to execute arbitrary code via a heap-based buffer overflow. Exploitation requires no user interaction and can occur through the Preview Pane, with low attack complexity and no privileges required.

#5 The Windows Graphics Component is also impacted by two critical vulnerabilities. CVE-2025-53800, an elevation of privilege flaw, allows authenticated local attackers with minimal privileges to escalate to SYSTEM by exploiting incorrect resource initialization.

#6 The attack is straightforward, requiring low complexity and no user interaction. Similarly, CVE-2025-55228, a remote code execution vulnerability in Windows Win32K - GRFX, involves a race condition that attackers must win to exploit. The flaw, affecting the graphical interface, could allow authenticated attackers to execute code remotely. These vulnerabilities highlight the pressing need for organizations to apply the latest security updates without delay.

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 Patch Deployment for High Risk and Publicly Disclosed Vulnerabilities. Special attention should be directed toward CVE-2025-55234 (Windows SMB), CVE-2024-21907 (Newtonsoft.Json), CVE-2025-54910 (Microsoft Office), and CVE-2025-55228 (Windows Graphics Component) due to their critical severity, public disclosure, and susceptibility to exploitation.

- Strengthen Authentication and Access Controls for systems with SMB Server configurations that lack signing or Extended Protection for Authentication (EPA), as well as environments using outdated NTLM protocols, are particularly vulnerable. Implement stronger authentication methods and enforce security policies wherever possible to enhance protection.

- Conduct Post-Patch Validation and Testing. After deploying patches, perform thorough testing to confirm that the vulnerabilities have been mitigated and that critical business functions remain operational without disruption.

All CVEs

CVE	NAME	PRODUCT	IMPACT
CVE-2025-47997	Microsoft SQL Server Information Disclosure Vulnerability	SQL Server	Information Disclosure
CVE-2025-49692	Azure Connected Machine Agent Elevation of Privilege Vulnerability	Azure Windows Virtual Machine Agent	Elevation of Privilege
CVE-2025-49734	PowerShell Direct Elevation of Privilege Vulnerability	Windows PowerShell	Elevation of Privilege
CVE-2025-53791	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2025-53796	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-53797	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-53798	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-53799	Windows Imaging Component Information Disclosure Vulnerability	Windows Imaging Component	Information Disclosure
CVE-2025-53800	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2025-53801	Microsoft DWM Core Library Elevation of Privilege Vulnerability	Windows DWM	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-53802	Windows Bluetooth Service Elevation of Privilege Vulnerability	Windows Bluetooth Service	Elevation of Privilege
CVE-2025-53803	Windows Kernel Memory Information Disclosure Vulnerability	Windows Kernel	Information Disclosure
CVE-2025-53804	Windows Kernel-Mode Driver Information Disclosure Vulnerability	Windows Kernel	Information Disclosure
CVE-2025-53805	HTTP.sys Denial of Service Vulnerability	Windows Internet Information Services	Denial of Service
CVE-2025-53806	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-53807	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2025-53808	Windows Defender Firewall Service Elevation of Privilege Vulnerability	Windows Defender Firewall Service	Elevation of Privilege
CVE-2025-53809	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability	Windows Local Security Authority Subsystem Service (LSASS)	Denial of Service
CVE-2025-53810	Windows Defender Firewall Service Elevation of Privilege Vulnerability	Windows Defender Firewall Service	Elevation of Privilege
CVE-2025-54091	Windows Hyper-V Elevation of Privilege Vulnerability	Role: Windows Hyper-V	Elevation of Privilege
CVE-2025-54092	Windows Hyper-V Elevation of Privilege Vulnerability	Role: Windows Hyper-V	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-54093	Windows TCP/IP Driver Elevation of Privilege Vulnerability	Windows TCP/IP	Elevation of Privilege
CVE-2025-54094	Windows Defender Firewall Service Elevation of Privilege Vulnerability	Windows Defender Firewall Service	Elevation of Privilege
CVE-2025-54095	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-54096	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-54097	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-54098	Windows Hyper-V Elevation of Privilege Vulnerability	Role: Windows Hyper-V	Elevation of Privilege
CVE-2025-54099	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-54101	Windows SMB Client Remote Code Execution Vulnerability	Windows SMBv3 Client	Remote Code Execution
CVE-2025-54102	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Windows Connected Devices Platform Service	Elevation of Privilege
CVE-2025-54103	Windows Management Service Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2025-54104	Windows Defender Firewall Service Elevation of Privilege Vulnerability	Windows Defender Firewall Service	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-54105	Microsoft Brokering File System Elevation of Privilege Vulnerability	Microsoft Brokering File System	Elevation of Privilege
CVE-2025-54106	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-54107	MapUrlToZone Security Feature Bypass Vulnerability	Windows MapUrlToZone	Security Feature Bypass
CVE-2025-54108	Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	Capability Access Management Service (camsvc)	Elevation of Privilege
CVE-2025-54109	Windows Defender Firewall Service Elevation of Privilege Vulnerability	Windows Defender Firewall Service	Elevation of Privilege
CVE-2025-54110	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2025-54111	Windows UI XAML Phone DatePickerFlyout Elevation of Privilege Vulnerability	Windows UI XAML Phone DatePickerFlyout	Elevation of Privilege
CVE-2025-54112	Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability	Microsoft Virtual Hard Drive	Elevation of Privilege
CVE-2025-54113	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-54114	Windows Connected Devices Platform Service (Cdpsvc) Denial of Service Vulnerability	Windows Connected Devices Platform Service	Denial of Service

CVE	NAME	PRODUCT	IMPACT
CVE-2025-54115	Windows Hyper-V Elevation of Privilege Vulnerability	Role: Windows Hyper-V	Elevation of Privilege
CVE-2025-54116	Windows MultiPoint Services Elevation of Privilege Vulnerability	Windows MultiPoint Services	Elevation of Privilege
CVE-2025-54894	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability	Windows Local Security Authority Subsystem Service (LSASS)	Elevation of Privilege
CVE-2025-54895	SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Elevation of Privilege Vulnerability	Windows SPNEGO Extended Negotiation	Elevation of Privilege
CVE-2025-54896	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-54897	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2025-54898	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-54899	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-54900	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-54901	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2025-54902	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-54903	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-54904	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-54905	Microsoft Word Information Disclosure Vulnerability	Microsoft Office Word	Information Disclosure
CVE-2025-54906	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-54907	Microsoft Office Visio Remote Code Execution Vulnerability	Microsoft Office Visio	Remote Code Execution
CVE-2025-54908	Microsoft PowerPoint Remote Code Execution Vulnerability	Microsoft Office PowerPoint	Remote Code Execution
CVE-2025-54910	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-54911	Windows BitLocker Elevation of Privilege Vulnerability	Windows BitLocker	Elevation of Privilege
CVE-2025-54912	Windows BitLocker Elevation of Privilege Vulnerability	Windows BitLocker	Elevation of Privilege
CVE-2025-54913	Windows UI XAML Maps MapControlSettings Elevation of Privilege Vulnerability	Windows UI XAML Maps MapControlSettings	Elevation of Privilege
CVE-2025-54915	Windows Defender Firewall Service Elevation of Privilege Vulnerability	Windows Defender Firewall Service	Elevation of Privilege
CVE-2025-54916	Windows NTFS Remote Code Execution Vulnerability	Windows NTFS	Remote Code Execution
CVE-2025-54917	MapUrlToZone Security Feature Bypass Vulnerability	Windows MapUrlToZone	Security Feature Bypass
CVE-2025-54918	Windows NTLM Elevation of Privilege Vulnerability	Windows NTLM	Elevation of Privilege
CVE-2025-54919	Windows Graphics Component Remote Code Execution Vulnerability	Windows Win32K - GRFX	Remote Code Execution
CVE-2025-55223	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Graphics Kernel	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-55224	Windows Hyper-V Remote Code Execution Vulnerability	Windows Win32K - GRFX	Remote Code Execution
CVE-2025-55225	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-55226	Graphics Kernel Remote Code Execution Vulnerability	Graphics Kernel	Remote Code Execution
CVE-2025-55227	Microsoft SQL Server Elevation of Privilege Vulnerability	SQL Server	Elevation of Privilege
CVE-2025-55228	Windows Graphics Component Remote Code Execution Vulnerability	Windows Win32K - GRFX	Remote Code Execution
CVE-2025-55232	Microsoft High Performance Compute (HPC) Pack Remote Code Execution Vulnerability	Microsoft High Performance Compute Pack (HPC)	Remote Code Execution
CVE-2025-55234	Windows SMB Elevation of Privilege Vulnerability	Windows SMB	Elevation of Privilege
CVE-2025-55236	Graphics Kernel Remote Code Execution Vulnerability	Graphics Kernel	Remote Code Execution
CVE-2025-55243	Microsoft OfficePlus Spoofing Vulnerability	Microsoft Office	Spoofing
CVE-2025-55245	Xbox Gaming Services Elevation of Privilege Vulnerability	XBox Gaming Services	Elevation of Privilege
CVE-2025-55316	Azure Connected Machine Agent Elevation of Privilege Vulnerability	Azure Connected Machine Agent	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-55317	Microsoft AutoUpdate (MAU) Elevation of Privilege Vulnerability	Microsoft AutoUpdate (MAU)	Elevation of Privilege
CVE-2024-21907	Newtonsoft.Json Denial of Service Vulnerability	SQL Server	Denial of Service
CVE-2025-9864	Google Chrome Use after free in V8 Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2025-9865	Google Chrome for Android UI Handling Domain Spoofing Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2025-9866	Google Chrome Content Security Policy Bypass Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2025-9867	Google Chrome for Android UI Spoofing Vulnerability	Microsoft Edge (Chromium-based)	Spoofing

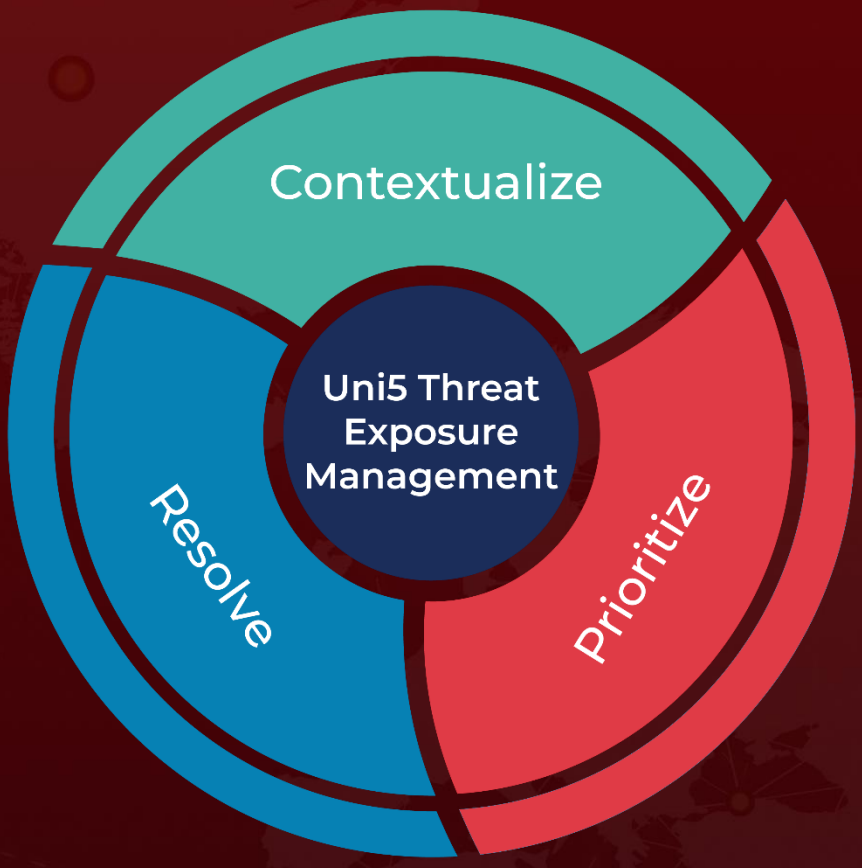
References

https://msrc.microsoft.com/update-guide/releaseNote/2025-Sep

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 11, 2025 . 6:00 AM

More at www.hivepro.com