

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Microsoft September 2025 Patch Tuesday Roundup

Date of Publication

September 11, 2025

Last Update Date

October 3, 2025

Admiralty Code

A1

TA Number

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	Chromium Use after free in V8 Vulnerability	Microsoft Edge (Chromium-based)			
CVE-2025-9866	Chromium Content Security Policy Bypass Vulnerability	Microsoft Edge (Chromium-based)			
<u>CVE-2025-10585</u>	Chromium Type Confusion in V8 Vulnerability	Microsoft Edge (Chromium-based)			

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





Potential MITRE ATT&CK TTPs

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



Vulnerability Details

#1

Microsoft's September 2025 Patch Tuesday delivers a significant security update, addressing a total of 91 vulnerabilities across its product ecosystem. Of these, 8 are classified as critical, 77 as important, and 1 as moderate in severity. The vulnerabilities span multiple categories: 41 elevation of privilege, 24 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 11 non-Microsoft CVEs, bringing the total to 97 vulnerabilities addressed this month. Importantly, 15 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.

#7

On September 11, 2025, and September 19, 2025, Microsoft released updates to the September 2025 Patch, addressing six vulnerabilities in the Chromium-based Microsoft Edge browser. The most critical of these was the zero-day vulnerability CVE-2025-10585. This flaw, resulting from a type confusion issue in the V8 JavaScript engine, is already being actively exploited. If left unpatched, it could enable attackers to cause system crashes or execute arbitrary code, posing a significant security threat.

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



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



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

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

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



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

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



CVE	NAME	PRODUCT	IMPACT
<u>CVE-2025-55224</u>	Windows Hyper-V Remote Code Execution Vulnerability	Windows Win32K - GRFX	Remote Code Execution
<u>CVE-2025-55225</u>	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
<u>CVE-2025-55226</u>	Graphics Kernel Remote Code Execution Vulnerability	Graphics Kernel	Remote Code Execution
<u>CVE-2025-55227</u>	Microsoft SQL Server Elevation of Privilege Vulnerability	SQL Server	Elevation of Privilege
<u>CVE-2025-55228</u>	Windows Graphics Component Remote Code Execution Vulnerability	Windows Win32K - GRFX	Remote Code Execution
<u>CVE-2025-55232</u>	Microsoft High Performance Compute (HPC) Pack Remote Code Execution Vulnerability	Microsoft High Performance Compute Pack (HPC)	Remote Code Execution
<u>CVE-2025-55234</u>	Windows SMB Elevation of Privilege Vulnerability	Windows SMB	Elevation of Privilege
<u>CVE-2025-55236</u>	Graphics Kernel Remote Code Execution Vulnerability	Graphics Kernel	Remote Code Execution
<u>CVE-2025-55243</u>	Microsoft OfficePlus Spoofing Vulnerability	Microsoft Office	Spoofing
<u>CVE-2025-55245</u>	Xbox Gaming Services Elevation of Privilege Vulnerability	XBox Gaming Services	Elevation of Privilege
<u>CVE-2025-55316</u>	Azure Connected Machine Agent Elevation of Privilege Vulnerability	Azure Connected Machine Agent	Elevation of Privilege
<u>CVE-2025-55317</u>	Microsoft AutoUpdate (MAU) Elevation of Privilege Vulnerability	Microsoft AutoUpdate (MAU)	Elevation of Privilege



CVE	NAME	PRODUCT	IMPACT
<u>CVE-2024-21907</u>	Newtonsoft.Json Denial of Service Vulnerability	SQL Server	Denial of Service
<u>CVE-2025-9864</u>	Chromium Use after free in V8 Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
<u>CVE-2025-9865</u>	Chromium Inappropriate implementation in Toolbar	Microsoft Edge (Chromium-based)	Spoofing
<u>CVE-2025-9866</u>	Chromium Content Security Policy Bypass Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
<u>CVE-2025-9867</u>	Chromium Inappropriate implementation in Downloads	Microsoft Edge (Chromium-based)	Spoofing
<u>CVE-2025-10200</u>	Chromium Use after free in Serviceworker Vulnerability	Microsoft Edge (Chromium-based)	Code Execution
<u>CVE-2025-10201</u>	Chromium Inappropriate implementation in Mojo	Microsoft Edge (Chromium-based)	Elevation of Privilege
<u>CVE-2025-10500</u>	Chromium Use after free in Dawn Vulnerability	Microsoft Edge (Chromium-based)	Code Execution
<u>CVE-2025-10501</u>	Chromium Use after free in WebRTC Vulnerability	Microsoft Edge (Chromium-based)	Code Execution
<u>CVE-2025-10502</u>	Chromium Heap buffer overflow in ANGLE Vulnerability	Microsoft Edge (Chromium-based)	Memory Corruption
<u>CVE-2025-10585</u>	Chromium Type Confusion in V8 Vulnerability	Microsoft Edge (Chromium-based)	Code Execution
<u>CVE-2025-55319</u>	Agentic AI and Visual Studio Code Remote Code Execution Vulnerability	Agentic AI and Visual Studio Code	Remote Code Execution
<u>CVE-2025-55322</u>	OmniParser Remote Code Execution Vulnerability	OmniParser	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
<u>CVE-2025-59215</u>	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
<u>CVE-2025-59216</u>	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
<u>CVE-2025-59220</u>	Windows Bluetooth Service Elevation of Privilege Vulnerability	Windows Bluetooth Service	Elevation of Privilege

References

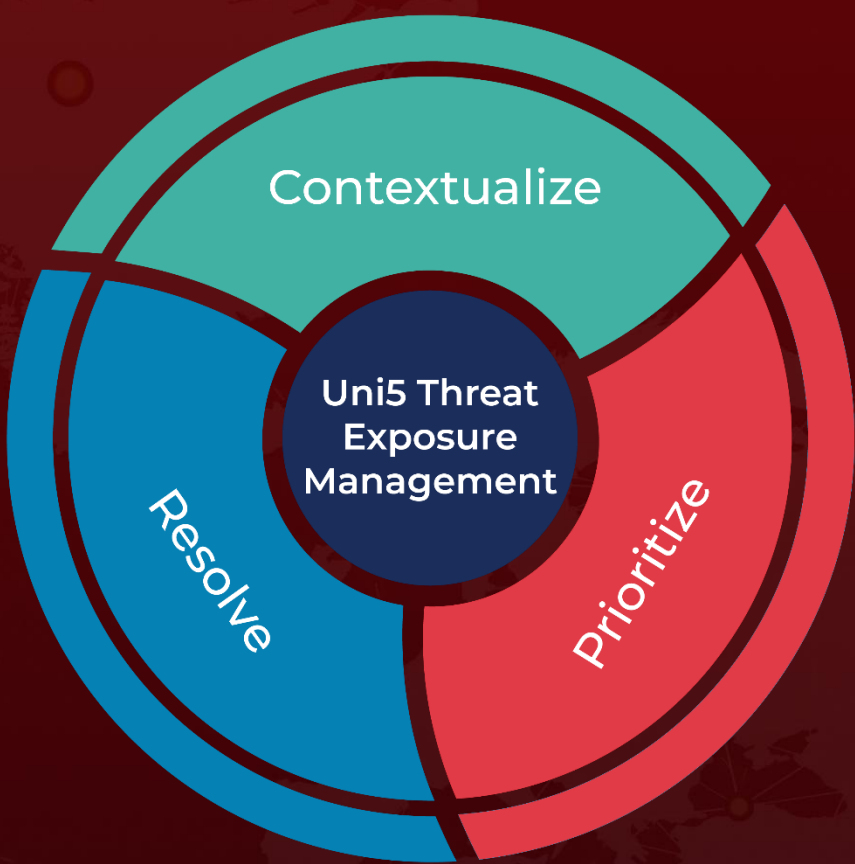
<https://msrc.microsoft.com/update-guide/releaseNote/2025-Sep>

<https://hivepro.com/threat-advisory/google-races-to-patch-chrome-sixth-zero-day-cve-2025-10585/>

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

