Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's August 2025 Patch Tuesday Roundup

Date of Publication	Admiralty Code	TA Number
August 14, 2025	A1	TA2025251

Summary

First Seen: August 12, 2025
Affected Platforms: Microsoft SQL Server, Windows Kerberos, Microsoft Exchange Server, Microsoft Office, Microsoft SharePoint, Google Chromium and more
Impact: Information Disclosure, Denial of Service, Remote Code Execution, Elevation of Privilege, Tampering, Spoofing

Exploitable CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-53779	BadSuccessor (Windows Kerberos Elevation of Privilege Vulnerability)	Windows Server 2025	✗	✗	✓
CVE-2025-49743	Windows Graphics Component Elevation of Privilege Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	✗	✗	✓
CVE-2025-50167	Windows Hyper-V Elevation of Privilege Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2012 - 2016	✗	✗	✓
CVE-2025-50168	Win32k Elevation of Privilege Vulnerability	Windows 11 24H2 Windows Server: 2022 - 2025	✗	✗	✓
CVE-2025-50177	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Windows Server: 2008 - 2012	✗	✗	✓
CVE-2025-53132	Win32k Elevation of Privilege Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-53147	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Server: 2008 - 2012	✗	✗	✓
CVE-2025-53156	Windows Storage Port Driver Information Disclosure Vulnerability	Windows 11 Version 24H2 Windows Server 2025	✗	✗	✓
CVE-2025-53778	Windows NTLM Elevation of Privilege Vulnerability	Windows: 10 - 11 23H2 Windows Server: 2012 - 2025	✗	✗	✓
CVE-2025-53786	Microsoft Exchange Server Hybrid Deployment Elevation of Privilege Vulnerability	Microsoft Exchange Server 2016 & 2019	✗	✗	✓
CVE-2025-48807	Windows Hyper-V Remote Code Execution Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2016 - 2022	✗	✗	✓
CVE-2025-49707	Azure Virtual Machines Spoofing Vulnerability	Azure Virtual Machines	✗	✗	✓
CVE-2025-50165	Windows Graphics Component Remote Code Execution Vulnerability	Windows 11 Version 24H2 Windows Server 2025	✗	✗	✓
CVE-2025-50176	DirectX Graphics Kernel Remote Code Execution Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2022 - 2025	✗	✗	✓
CVE-2025-53733	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office 2019 Microsoft SharePoint Server: 2016 - 2019 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise Microsoft Word 2016	✗	✗	✓
CVE-2025-53740	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office 2016 & 2019 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-53766	GDI+ Remote Code Execution Vulnerability	Windows: 10 - 11 24H2 Windows Server 2008 - 2025	✗	✗	✓
CVE-2025-53767	Azure OpenAI Elevation of Privilege Vulnerability	Azure Open AI	✗	✗	✓
CVE-2025-53774	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability	Microsoft 365 Copilot's Business Chat	✗	✗	✓
CVE-2025-53781	Azure Virtual Machines Information Disclosure Vulnerability	Azure Virtual Machines	✗	✗	✓
CVE-2025-53787	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability	Microsoft 365 Copilot's Business Chat	✗	✗	✓

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0006 Credential Access	TA0005 Defense Evasion	TA0040 Impact	T1566 Phishing
T1588 Obtain Capabilities	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities
T1588.005 Exploits	T1078 Valid Accounts	T1203 Exploitation for Client Execution	T1556 Modify Authentication Process
T1558 Steal or Forge Kerberos Tickets	T1068 Exploitation for Privilege Escalation	T1550.003 Pass the Ticket	T1550 Use Alternate Authentication Material
T1499 Endpoint Denial of Service	T1210 Exploitation of Remote Services		

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

Vulnerability Details

#1

Microsoft's August 2025 Patch Tuesday delivers an extensive batch of security updates, addressing 111 vulnerabilities across its product ecosystem. These include 17 rated Critical, 91 Important, two Moderate, and one Low in severity. The vulnerabilities span various categories: 35 Remote Code Execution (RCE), 44 Elevation of Privilege, 18 Information Disclosure, 4 Denial of Service, 9 Spoofing, and 1 Tampering issue. Beyond its own products, Microsoft also released patches for 8 non-Microsoft CVEs, pushing the total count of vulnerabilities addressed this month to 119. Notably, 21 of these CVEs are considered at risk of exploitation, underscoring the urgency of prompt patch deployment.

#2

The most high-profile fix this month was the publicly disclosed flaw CVE-2025-53779, nicknamed "BadSuccessor", a Kerberos EoP vulnerability involving relative path traversal in delegated Managed Service Accounts (dMSAs). Although rated Moderate, the bug is dangerous in enterprise contexts, as it could enable attackers with elevated privileges to escalate to domain administrator level. However, exploitation is somewhat constrained by the requirement for access to privileged dMSA (delegated Managed Service Account) attributes, which narrows the pool of potential attackers.

#3

Critical vulnerabilities this month include CVE-2025-53786, an Exchange Server Hybrid EoP flaw that could let attackers with on-premises Exchange admin rights pivot into Office 365 or Exchange Online, potentially compromising cloud accounts; CVE-2025-53778, a Windows NTLM EoP flaw (CVSS 8.8) flagged as "Exploitation More Likely"; and CVE-2025-50177, a Microsoft Message Queuing (MSMQ) RCE vulnerability that could be triggered via crafted network packets.

#4

Also noteworthy are CVE-2025-53766 (a GDI+ heap overflow RCE) and CVE-2025-50165 (a Graphics Component RCE via malicious JPEG rendering). These highlight the variety of attack surfaces covered this month, from core Windows networking protocols to database and cloud-connected systems.

#5

This update also serves as a reminder that Windows 10 will lose free security updates after October 14, 2025, making timely patching even more important as systems near end-of-support. The mix of privilege escalation, RCE, and hybrid-cloud attack vectors in August's release reinforces the importance of timely, prioritized patching.

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 publicly disclosed and critical vulnerabilities CVE-2025-53779, CVE-2025-53786, CVE-2025-53778, CVE-2025-50177, CVE-2025-53766, CVE-2025-50165. 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.

All CVEs

CVE	NAME	PRODUCT	IMPACT
CVE-2025-24999	Microsoft SQL Server Elevation of Privilege Vulnerability	Microsoft SQL Server	Elevation of Privilege
CVE-2025-25005	Microsoft Exchange Server Tampering Vulnerability	Microsoft Exchange Server	Tampering
CVE-2025-25006	Microsoft Exchange Server Spoofing Vulnerability	Microsoft Exchange Server	Spoofing
CVE-2025-25007	Microsoft Exchange Server Spoofing Vulnerability	Microsoft Exchange Server	Spoofing
CVE-2025-33051	Microsoft Exchange Server Information Disclosure Vulnerability	Microsoft Exchange Server	Information Disclosure
CVE-2025-47954	Microsoft SQL Server Elevation of Privilege Vulnerability	Microsoft SQL Server	Elevation of Privilege
CVE-2025-48807	Windows Hyper-V Remote Code Execution Vulnerability	Windows Hyper-V	Remote Code Execution
CVE-2025-49707	Azure Virtual Machines Spoofing Vulnerability	Azure Virtual Machines	Spoofing
CVE-2025-49712	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	Remote Code Execution
CVE-2025-49736	Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability	Microsoft Edge (Chromium-based)	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2025-49743	Windows Graphics Component Elevation of Privilege Vulnerability	Windows Graphics Component	Elevation of Privilege
CVE-2025-49745	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	Microsoft Dynamics 365 (on-premises)	Spoofing
CVE-2025-49751	Windows Hyper-V Denial of Service Vulnerability	Windows Hyper-V Denial	Denial of Service
CVE-2025-49755	Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2025-49757	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49758	Microsoft SQL Server Elevation of Privilege Vulnerability	Microsoft SQL Server	Elevation of Privilege
CVE-2025-49759	Microsoft SQL Server Elevation of Privilege Vulnerability	Microsoft SQL Server	Elevation of Privilege
CVE-2025-49761	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2025-49762	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-50153	Desktop Windows Manager Elevation of Privilege Vulnerability	Desktop Windows Manager	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-50154	Microsoft Windows File Explorer Spoofing Vulnerability	Microsoft Windows File	Spoofing
CVE-2025-50155	Windows Push Notifications Apps Elevation of Privilege Vulnerability	Windows Push Notifications Apps	Elevation of Privilege
CVE-2025-50156	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-50157	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-50158	Windows NTFS Information Disclosure Vulnerability	Windows NTFS	Information Disclosure
CVE-2025-50159	Remote Access Point-to-Point Protocol (PPP) EAP-TLS Elevation of Privilege Vulnerability	Remote Access Point-to-Point Protocol (PPP) EAP-TLS	Elevation of Privilege
CVE-2025-50160	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-50161	Win32k Elevation of Privilege Vulnerability	Windows Win32k	Elevation of Privilege
CVE-2025-50162	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-50163	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-50164	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-50165	Windows Graphics Component Remote Code Execution Vulnerability	Windows Graphics Component	Remote Code Execution
CVE-2025-50166	Windows Distributed Transaction Coordinator (MSDTC) Information Disclosure Vulnerability	Windows Distributed Transaction Coordinator (MSDTC)	Information Disclosure
CVE-2025-50167	Windows Hyper-V Elevation of Privilege Vulnerability	Windows Hyper-V	Elevation of Privilege
CVE-2025-50168	Win32k Elevation of Privilege Vulnerability	Windows Win32k	Elevation of Privilege
CVE-2025-50169	Windows SMB Remote Code Execution Vulnerability	Windows SMB	Remote Code Execution
CVE-2025-50170	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver	Elevation of Privilege
CVE-2025-50171	Remote Desktop Spoofing Vulnerability	Remote Desktop	Spoofing
CVE-2025-50172	DirectX Graphics Kernel Denial of Service Vulnerability	DirectX Graphics Kernel	Denial of Service
CVE-2025-50173	Windows Installer Elevation of Privilege Vulnerability	Windows Installer	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-50176	DirectX Graphics Kernel Remote Code Execution Vulnerability	DirectX Graphics Kernel	Remote Code Execution
CVE-2025-50177	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Microsoft Message Queuing (MSMQ)	Remote Code Execution
CVE-2025-53131	Windows Media Remote Code Execution Vulnerability	Windows Media	Remote Code Execution
CVE-2025-53132	Win32k Elevation of Privilege Vulnerability	Windows Win32k	Elevation of Privilege
CVE-2025-53133	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Windows PrintWorkflowUserSvc	Elevation of Privilege
CVE-2025-53134	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-53135	DirectX Graphics Kernel Elevation of Privilege Vulnerability	DirectX Graphics Kernel	Elevation of Privilege
CVE-2025-53136	NT OS Kernel Information Disclosure Vulnerability	NT OS Kernel	Information Disclosure
CVE-2025-53137	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-53138	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2025-53140	Windows Kernel Transaction Manager Elevation of Privilege Vulnerability	Windows Kernel Transaction Manager	Elevation of Privilege
CVE-2025-53141	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-53142	Microsoft Brokering File System Elevation of Privilege Vulnerability	Microsoft Brokering File System	Elevation of Privilege
CVE-2025-53143	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Microsoft Message Queuing (MSMQ)	Remote Code Execution
CVE-2025-53144	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Microsoft Message Queuing (MSMQ)	Remote Code Execution
CVE-2025-53145	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Microsoft Message Queuing (MSMQ)	Remote Code Execution
CVE-2025-53147	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-53148	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-53149	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Kernel Streaming WOW Thunk Service Driver	Elevation of Privilege
CVE-2025-53151	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2025-53152	Desktop Windows Manager Remote Code Execution Vulnerability	Desktop Windows Manager	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-53153	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-53154	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-53155	Windows Hyper-V Elevation of Privilege Vulnerability	Windows Hyper-V	Elevation of Privilege
CVE-2025-53156	Windows Storage Port Driver Information Disclosure Vulnerability	Windows Storage Port Driver	Information Disclosure
CVE-2025-53716	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability	Local Security Authority Subsystem Service (LSASS)	Denial of Service
CVE-2025-53718	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-53719	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-53720	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-53721	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Windows Connected Devices Platform Service	Elevation of Privilege
CVE-2025-53722	Windows Remote Desktop Services Denial of Service Vulnerability	Windows Remote Desktop Services	Denial of Service

CVE	NAME	PRODUCT	IMPACT
CVE-2025-53723	Windows Hyper-V Elevation of Privilege Vulnerability	Windows Hyper-V Elevation	Elevation of Privilege
CVE-2025-53724	Windows Push Notifications Apps Elevation of Privilege Vulnerability	Windows Push Notifications Apps	Elevation of Privilege
CVE-2025-53725	Windows Push Notifications Apps Elevation of Privilege Vulnerability	Windows Push Notifications Apps	Elevation of Privilege
CVE-2025-53726	Windows Push Notifications Apps Elevation of Privilege Vulnerability	Windows Push Notifications Apps	Elevation of Privilege
CVE-2025-53727	Microsoft SQL Server Elevation of Privilege Vulnerability	Microsoft SQL Server	Elevation of Privilege
CVE-2025-53728	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	Microsoft Dynamics 365 (On-Premises)	Information Disclosure
CVE-2025-53729	Microsoft Azure File Sync Elevation of Privilege Vulnerability	Microsoft Azure File Sync	Elevation of Privilege
CVE-2025-53730	Microsoft Office Visio Remote Code Execution Vulnerability	Microsoft Office Visio	Remote Code Execution
CVE-2025-53731	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-53732	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-53733	Microsoft Word Remote Code Execution Vulnerability	Microsoft Word	Remote Code Execution
CVE-2025-53734	Microsoft Office Visio Remote Code Execution Vulnerability	Microsoft Office Visio	Remote Code Execution
CVE-2025-53735	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Excel	Remote Code Execution
CVE-2025-53736	Microsoft Word Information Disclosure Vulnerability	Microsoft Word	Information Disclosure
CVE-2025-53737	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Excel	Remote Code Execution
CVE-2025-53738	Microsoft Word Remote Code Execution Vulnerability	Microsoft Word	Remote Code Execution
CVE-2025-53739	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Excel	Remote Code Execution
CVE-2025-53740	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-53741	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Excel	Remote Code Execution
CVE-2025-53759	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Excel	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-53760	Microsoft SharePoint Elevation of Privilege Vulnerability	Microsoft SharePoint	Elevation of Privilege
CVE-2025-53761	Microsoft PowerPoint Remote Code Execution Vulnerability	Microsoft PowerPoint	Remote Code Execution
CVE-2025-53765	Azure Stack Hub Information Disclosure Vulnerability	Azure Stack Hub	Information Disclosure
CVE-2025-53766	GDI+ Remote Code Execution Vulnerability	GDI+	Remote Code Execution
CVE-2025-53767	Azure OpenAI Elevation of Privilege Vulnerability	Azure OpenAI	Elevation of Privilege
CVE-2025-53769	Windows Security App Spoofing Vulnerability	Windows Security App	Spoofing
CVE-2025-53772	Web Deploy Remote Code Execution Vulnerability	Web Deploy	Remote Code Execution
CVE-2025-53773	GitHub Copilot and Visual Studio Remote Code Execution Vulnerability	GitHub Copilot and Visual Studio	Remote Code Execution
CVE-2025-53774	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability	Microsoft 365 Copilot BizChat	Information Disclosure
CVE-2025-53778	Windows NTLM Elevation of Privilege Vulnerability	Windows NTLM	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-53779	Windows Kerberos Elevation of Privilege Vulnerability	Windows Kerberos	Elevation of Privilege
CVE-2025-53781	Azure Virtual Machines Information Disclosure Vulnerability	Azure Virtual Machines	Information Disclosure
CVE-2025-53783	Microsoft Teams Remote Code Execution Vulnerability	Microsoft Teams	Remote Code Execution
CVE-2025-53784	Microsoft Word Remote Code Execution Vulnerability	Microsoft Word	Remote Code Execution
CVE-2025-53786	Microsoft Exchange Server Hybrid Deployment Elevation of Privilege Vulnerability	Microsoft Exchange Server	Elevation of Privilege
CVE-2025-53787	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability	Microsoft 365 Copilot BizChat	Information Disclosure
CVE-2025-53788	Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability	Windows Subsystem for Linux (WSL2) Kernel	Elevation of Privilege
CVE-2025-53789	Windows StateRepository API Server file Elevation of Privilege Vulnerability	Windows StateRepository API Server file	Elevation of Privilege
CVE-2025-53792	Azure Portal Elevation of Privilege Vulnerability	Azure Portal	Elevation of Privilege
CVE-2025-53793	Azure Stack Hub Information Disclosure Vulnerability	Azure Stack Hub	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2025-8576	Google Chromium Use After Free Vulnerability	Google Chromium	Heap Corruption
CVE-2025-8577	Google Chromium Inappropriate Implementation in Picture In Picture Vulnerability	Google Chromium	Spoofing
CVE-2025-8578	Google Chromium Use After Free Vulnerability	Google Chromium	Heap Corruption
CVE-2025-8579	Google Chromium Inappropriate Implementation in Gemini Live Vulnerability	Google Chromium	Spoofing
CVE-2025-8580	Google Chromium Inappropriate Implementation in Filesystems Vulnerability	Google Chromium	Spoofing
CVE-2025-8581	Google Chromium Inappropriate Implementation in Extensions Vulnerability	Google Chromium	Spoofing
CVE-2025-8582	Google Chromium Insufficient Validation of Untrusted input in DOM Vulnerability	Google Chromium	Spoofing
CVE-2025-8583	Google Chromium Inappropriate Implementation in Permissions Vulnerability	Google Chromium	Spoofing

References

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

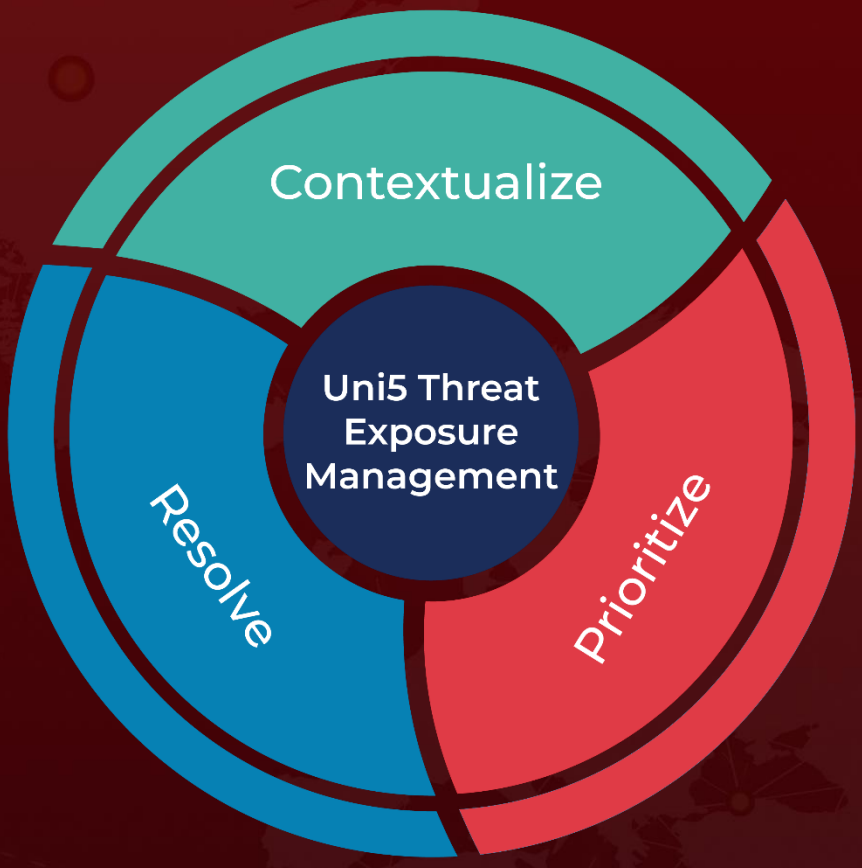
https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory

https://support.microsoft.com/en-us/windows/windows-10-support-ends-on-october-14-2025-2ca8b313-1946-43d3-b55c-2b95b107f281

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

August 14, 2025 • 9:30 AM

More at www.hivepro.com