Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft’s November 2025 Patch Tuesday Roundup

Date of Publication	Admiralty Code	TA Number
November 13, 2025	A1	TA2025345

Summary

First Seen: November 11, 2025
Affected Platforms: Microsoft Windows, Microsoft SQL Server, Microsoft Exchange Server, Microsoft Office, Microsoft SharePoint, Microsoft Edge and more
Impact: Information Disclosure, Denial of Service, Remote Code Execution, Elevation of Privilege, Spoofing, Security Feature Bypass

Exploitable CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-62215	Windows Kernel Elevation of Privilege Vulnerability	Windows: 10 - 11 25H2 Windows Server: 2019 - 2025	✓	✓	✓
CVE-2025-59512	Customer Experience Improvement Program (CEIP) Elevation of Privilege Vulnerability	Windows: 10 - 11 25H2 Windows Server: 2016 - 2025	✗	✗	✓
CVE-2025-60705	Windows Client-Side Caching Elevation of Privilege Vulnerability	Windows: 10 - 11 25H2 Windows Server: 2008 - 2025	✗	✗	✓
CVE-2025-60719	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows: 10 - 11 25H2 Windows Server: 2008 - 2025	✗	✗	✓
CVE-2025-62213	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows: 10 - 11 25H2 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-2025-62217	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows: 10 - 11 25H2 Windows Server: 2008 - 2025	✗	✗	✓
CVE-2025-30398	Nuance PowerScribe 360 Information Disclosure Vulnerability	Nuance PowerScribe 360 Nuance PowerScribe One	✗	✗	✓
CVE-2025-60716	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Windows: 10 - 11 25H2 Windows Server: 2019 - 2025	✗	✗	✓
CVE-2025-60724	GDI+ Remote Code Execution Vulnerability	Windows: 10 - 11 25H2 Windows Server: 2008 - 2025 Microsoft Office LTSC for Mac 2024 & 2021 Microsoft Office for Android	✗	✗	✓
CVE-2025-62199	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office LTSC for Mac 2024 & 2021 Microsoft Office 2016 Microsoft Office LTSC 2021 & 2024 Microsoft Office for Android Microsoft 365 Apps for Enterprise	✗	✗	✓
CVE-2025-62214	Visual Studio Remote Code Execution Vulnerability	Microsoft Visual Studio 2022 version 17.14	✗	✗	✓

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

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
T1499 Endpoint Denial of Service	T1068 Exploitation for Privilege Escalation	T1210 Exploitation of Remote Services	T1550 Use Alternate Authentication Material
T1557 Adversary-in-the-Middle	T1204 User Execution		

Vulnerability Details

#1

Microsoft's November 2025 Patch Tuesday delivers an extensive batch of security updates, addressing 63 vulnerabilities across its product ecosystem. These include 5 rated Critical, and 58 Important in severity. The vulnerabilities span various categories: 16 Remote Code Execution (RCE), 29 Elevation of Privilege, 11 Information Disclosure, 3 Denial of Service, 2 Spoofing, and 2 Security Feature Bypass issue. Beyond its own products, Microsoft also released patches for 5 non-Microsoft CVEs, pushing the total count of vulnerabilities addressed this month to 68. Notably, 11 of these CVEs are considered at risk of exploitation, underscoring the urgency of prompt patch deployment.

#2

The most pressing concern is the zero-day vulnerability CVE-2025-62215, an Elevation of Privilege (EoP) flaw in the Windows Kernel that is actively exploited in the wild. While this issue requires attackers to already have local, authenticated access, successful exploitation grants SYSTEM-level privileges, effectively allowing full control over a compromised host. Immediate patch deployment is strongly recommended to disrupt these attack chains and maintain endpoint integrity.

#3

Beyond the zero-day, several vulnerabilities were rated Critical due to their potential to allow Remote Code Execution (RCE). CVE-2025-60724, affecting the Microsoft Graphics Component (GDI+), poses a severe threat as it can be triggered by tricking users into opening a malicious image or document. Likewise, CVE-2025-62199, a critical RCE in Microsoft Office, could be exploited through specially crafted Office files, making it a key risk for organizations with email-driven workflows. Another critical issue, CVE-2025-62214, impacts Visual Studio, and could be abused to execute arbitrary code when malicious projects are opened.

#4

Several Elevation of Privilege vulnerabilities, such as CVE-2025-59512, CVE-2025-60705, and CVE-2025-60719, affect Windows subsystems like the Client-Side Caching Service and the Ancillary Function Driver for WinSock, with Microsoft assessing exploitation as “more likely.” These issues may be leveraged by attackers post-compromise to escalate privileges and maintain persistence.

#5

This update is marked by a critical zero-day and multiple RCE flaws affecting Windows and Microsoft applications. As this is the first update after Windows 10’s end of support (October 14, 2025), organizations must ensure ESU enrollment to stay protected. Immediate patching of CVE-2025-62215 and CVE-2025-60724, along with other critical updates, is strongly recommended to maintain system security and compliance.

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-2025-62215, CVE-2025-60724, CVE-2025-62199, and CVE-2025-62214. 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.

Ensure Windows 10 ESU compliance, verify all Windows 10 systems are enrolled in the Extended Security Update (ESU) program or upgrade to Windows 11 to maintain protection beyond October 2025.

All CVEs

CVE	NAME	PRODUCT	IMPACT
CVE-2025-30398	Nuance PowerScribe 360 Information Disclosure Vulnerability	Nuance PowerScribe	Information Disclosure
CVE-2025-47179	Configuration Manager Elevation of Privilege Vulnerability	Microsoft Configuration Manager	Elevation of Privilege
CVE-2025-59240	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2025-59499	Microsoft SQL Server Elevation of Privilege Vulnerability	Microsoft SQL Server	Elevation of Privilege
CVE-2025-59504	Azure Monitor Agent Remote Code Execution Vulnerability	Azure Monitor Agent	Remote Code Execution
CVE-2025-59505	Windows Smart Card Reader Elevation of Privilege Vulnerability	Windows Smart Card	Elevation of Privilege
CVE-2025-59506	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Windows DirectX	Elevation of Privilege
CVE-2025-59507	Windows Speech Runtime Elevation of Privilege Vulnerability	Windows Speech	Elevation of Privilege
CVE-2025-59508	Windows Speech Recognition Elevation of Privilege Vulnerability	Windows Speech	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59509	Windows Speech Recognition Information Disclosure Vulnerability	Windows Speech	Information Disclosure
CVE-2025-59510	Windows Routing and Remote Access Service (RRAS) Denial of Service Vulnerability	Windows Routing and Remote Access Service (RRAS)	Denial of Service
CVE-2025-59511	Windows WLAN Service Elevation of Privilege Vulnerability	Windows WLAN Service	Elevation of Privilege
CVE-2025-59512	Customer Experience Improvement Program (CEIP) Elevation of Privilege Vulnerability	Customer Experience Improvement Program (CEIP)	Elevation of Privilege
CVE-2025-59513	Windows Bluetooth RFCOM Protocol Driver Information Disclosure Vulnerability	Windows Bluetooth RFCOM Protocol Driver	Information Disclosure
CVE-2025-59514	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability	Microsoft Streaming Service	Elevation of Privilege
CVE-2025-59515	Windows Broadcast DVR User Service Elevation of Privilege Vulnerability	Windows Broadcast DVR User Service	Elevation of Privilege
CVE-2025-60703	Windows Remote Desktop Services Elevation of Privilege Vulnerability	Windows Remote Desktop	Elevation of Privilege
CVE-2025-60704	Windows Kerberos Elevation of Privilege Vulnerability	Windows Kerberos	Elevation of Privilege
CVE-2025-60705	Windows Client-Side Caching Elevation of Privilege Vulnerability	Windows Client-Side Caching (CSC) Service	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-60706	Windows Hyper-V Information Disclosure Vulnerability	Windows Hyper-V	Information Disclosure
CVE-2025-60707	Multimedia Class Scheduler Service (MMCSS) Driver Elevation of Privilege Vulnerability	Multimedia Class Scheduler Service (MMCSS)	Elevation of Privilege
CVE-2025-60708	Storvsp.sys Driver Denial of Service Vulnerability	Storvsp.sys Driver	Denial of Service
CVE-2025-60709	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	Elevation of Privilege
CVE-2025-60710	Host Process for Windows Tasks Elevation of Privilege Vulnerability	Host Process for Windows Tasks	Elevation of Privilege
CVE-2025-60713	Windows Routing and Remote Access Service (RRAS) Elevation of Privilege Vulnerability	Windows Routing and Remote Access Service (RRAS)	Elevation of Privilege
CVE-2025-60714	Windows OLE Remote Code Execution Vulnerability	Windows OLE	Remote Code Execution
CVE-2025-60715	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-60716	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Windows DirectX	Elevation of Privilege
CVE-2025-60717	Windows Broadcast DVR User Service Elevation of Privilege Vulnerability	Windows Broadcast DVR User Service	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-60718	Windows Administrator Protection Elevation of Privilege Vulnerability	Windows Administrator Protection	Elevation of Privilege
CVE-2025-60719	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-60720	Windows Transport Driver Interface (TDI) Translation Driver Elevation of Privilege Vulnerability	Windows TDX.sys	Elevation of Privilege
CVE-2025-60721	Windows Administrator Protection Elevation of Privilege Vulnerability	Windows Administrator Protection	Elevation of Privilege
CVE-2025-60722	Microsoft OneDrive for Android Elevation of Privilege Vulnerability	OneDrive for Android	Elevation of Privilege
CVE-2025-60723	DirectX Graphics Kernel Denial of Service Vulnerability	Windows DirectX	Denial of Service
CVE-2025-60724	GDI+ Remote Code Execution Vulnerability	Microsoft Graphics Component	Remote Code Execution
CVE-2025-60726	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2025-60727	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-60728	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2025-62199	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-62200	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-62201	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-62202	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2025-62203	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-62204	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2025-62205	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2025-62206	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	Microsoft Dynamics 365 (on-premises)	Information Disclosure
CVE-2025-62208	Windows License Manager Information Disclosure Vulnerability	Windows License Manager	Information Disclosure
CVE-2025-62209	Windows License Manager Information Disclosure Vulnerability	Windows License Manager	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2025-62210	Dynamics 365 Field Service (online) Spoofing Vulnerability	Dynamics 365 Field Service (online)	Spoofing
CVE-2025-62211	Dynamics 365 Field Service (online) Spoofing Vulnerability	Dynamics 365 Field Service (online)	Spoofing
CVE-2025-62213	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-62214	Visual Studio Remote Code Execution Vulnerability	Visual Studio	Remote Code Execution
CVE-2025-62215	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2025-62216	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-62217	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-62218	Microsoft Wireless Provisioning System Elevation of Privilege Vulnerability	Microsoft Wireless Provisioning System	Elevation of Privilege
CVE-2025-62219	Microsoft Wireless Provisioning System Elevation of Privilege Vulnerability	Microsoft Wireless Provisioning System	Elevation of Privilege
CVE-2025-62220	Windows Subsystem for Linux GUI Remote Code Execution Vulnerability	Windows Subsystem for Linux GUI	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-62222	Agentic AI and Visual Studio Code Remote Code Execution Vulnerability	Visual Studio Code CoPilot Chat Extension	Remote Code Execution
CVE-2025-62449	Microsoft Visual Studio Code CoPilot Chat Extension Security Feature Bypass Vulnerability	Visual Studio Code CoPilot Chat Extension	Security Feature Bypass
CVE-2025-62452	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-62453	GitHub Copilot and Visual Studio Code Security Feature Bypass Vulnerability	GitHub Copilot and Visual Studio Code	Security Feature Bypass
CVE-2025-12725	Chromium Out of bounds write in WebGPU Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2025-12726	Chromium Inappropriate implementation in Views Vulnerability	Microsoft Edge (Chromium-based)	Elevation of Privilege
CVE-2025-12727	Chromium Inappropriate implementation in V8 Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2025-12728	Chromium Inappropriate implementation in Omnibox Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2025-12729	Chromium Inappropriate implementation in Omnibox Vulnerability	Microsoft Edge (Chromium-based)	Spoofing

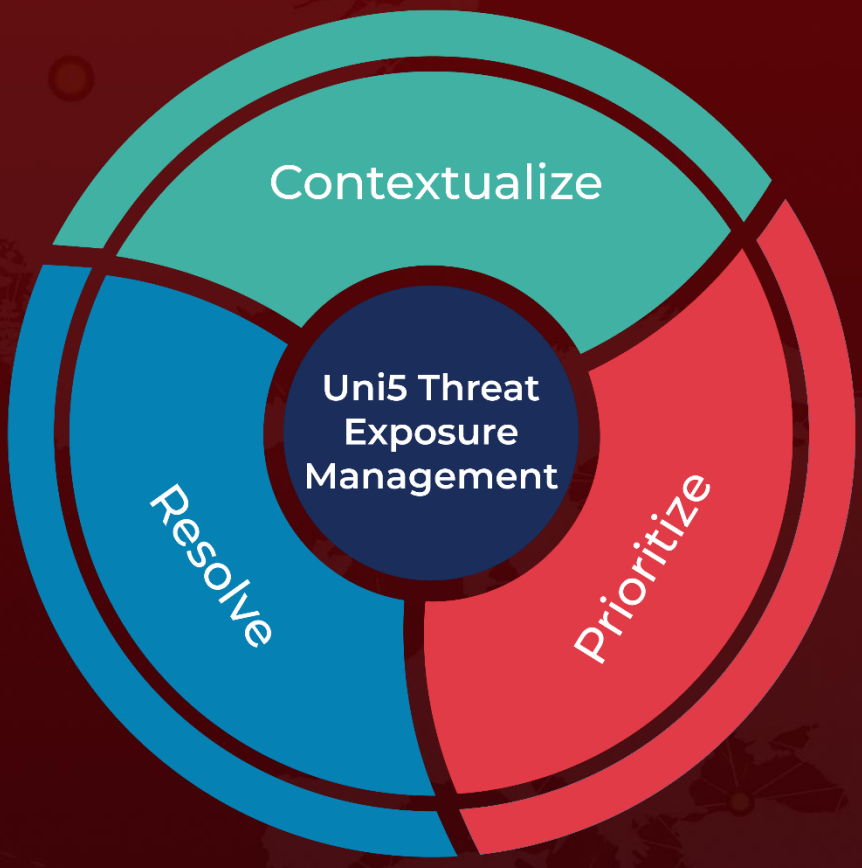
References

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

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

November 13, 2025 . 9:30 AM

More at www.hivepro.com