Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's October 2025 Patch Tuesday

Date of Publication	Admiralty Code	TA Number
October 16, 2025	A1	TA2025317

Summary

First Seen: October 14, 2025
Affected Platforms: Agere Windows Modem Driver, Microsoft Brokering File System, Windows USB Video Driver, Windows DWM, Windows Error Reporting, Azure Entra ID, Windows Server 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, Tampering

Exploitable CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-59230	Microsoft Windows Improper Access Control Vulnerability	Windows Server 2008, 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	✓	✓	✓
CVE-2025-47827	IGEL OS Use of a Key Past its Expiration Date Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	✓	✓	✓
CVE-2025-24990	Microsoft Windows Untrusted Pointer Dereference Vulnerability	Windows Server 2008, 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	✓	✓	✓
CVE-2025-24052	Windows Agere Modem Driver Elevation of Privilege Vulnerability	Windows Server 2008, 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	✗	✗	✓
CVE-2025-48004	Microsoft Brokering File System Elevation of Privilege Vulnerability	Windows Server 2022, 2025; Windows 11 25H2	✗	✗	✓
CVE-2025-55676	Windows USB Video Class System Driver Information Disclosure Vulnerability	Windows Server 2025; Windows 11 25H2	✗	✗	✓
CVE-2025-55680	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Server 2019, 2022, 2025; Windows 10 - 11 25H2	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-55681	Desktop Windows Manager Elevation of Privilege Vulnerability	Windows Server 2019, 2022, 2025; Windows 10 - 11 25H2	✗	✗	✓
CVE-2025-55692	Windows Error Reporting Service Elevation of Privilege Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	✗	✗	✓
CVE-2025-55693	Windows Kernel Elevation of Privilege Vulnerability	Windows Server 2025;Windows 11 25H2	✗	✗	✓
CVE-2025-55694	Windows Error Reporting Service Elevation of Privilege Vulnerability	Windows Server 2022, 2025; Windows 11 25H2	✗	✗	✓
CVE-2025-58722	Microsoft DWM Core Library Elevation of Privilege Vulnerability	Windows Server 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	✗	✗	✓
CVE-2025-59194	Windows Kernel Elevation of Privilege Vulnerability	Windows Server 2022, 2025; Windows 11 Version 25H2	✗	✗	✓
CVE-2025-59199	Software Protection Platform (SPP) Elevation of Privilege Vulnerability	Windows Server 2019, 2022, 2025; Windows 10 - 11 25H2	✗	✗	✓
CVE-2025-59246	Azure Entra ID Elevation of Privilege Vulnerability	Microsoft Entra ID	✗	✗	✓
CVE-2025-59287	Windows Server Update Service (WSUS) Remote Code Execution Vulnerability	Windows Server 2012, 2016, 2019, 2022, 2025	✗	✗	✓
CVE-2025-59502	Remote Procedure Call Denial of Service Vulnerability	Windows Server 2019, 2022, 2025; Windows 10 - 11 24H2	✗	✗	✓
CVE-2025-0033	AMD Improper Access Control Vulnerability	Azure Confidential Compute VM SKU ECasv5/ECadsv5, ECasv6/ECadsv6; Azure Confidential Compute VM SKU DCasv5/DCadsv5, DCasv6/DCadsv6; Azure Confidential Compute GPU SKU NCC40ads_H100_v5	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-2884	TCG TPM2.0 Reference Implementation Out-of-Bounds Read Vulnerability	Windows Server 2022, 2025; Windows 11 25H2	✗	✗	✓
CVE-2025-59489	Unity Gaming Engine Editor Vulnerability	Unity Gaming Engine Editor	✗	✗	✓

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0007** Discovery	**TA0040** Impact
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1190** Exploit Public-Facing Application	**T1566** Phishing
T1059 Command and Scripting Interpreter	**T1203** Exploitation for Client Execution	**T1068** Exploitation for Privilege Escalation	**T1547** Boot or Logon Autostart Execution
T1548 Abuse Elevation Control Mechanism	**T1055** Process Injection	**T1498** Network Denial of Service	**T1070** Indicator Removal
T1083 File and Directory Discovery	**T1553** Subvert Trust Controls		

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

Vulnerability Details

#1

Microsoft's October 2025 Patch Tuesday brings a substantial security refresh, addressing 175 vulnerabilities across its product ecosystem. Of these, 15 are critical, 158 important, and 2 moderate in severity. The vulnerabilities span a wide range of categories: 84 elevation of privilege, 29 remote code execution (RCE), 26 information disclosure, 11 denial of service, 10 security feature bypass, 1 tampering, and 14 spoofing issues. In addition, Microsoft has patched 21 non-Microsoft CVEs, bringing this month's total to 196 vulnerabilities. Notably, 20 of these flaws are actively at risk of exploitation, underscoring the urgent need for prompt patch deployment.

#2

This month's updates include patches for exploited vulnerabilities, with new zero-day flaws being reported. One key exploited flaw, CVE-2025-24990, affects the Windows Agere Modem Driver. Exploitation could grant attackers administrator privileges. The vulnerable driver has been removed in this October cumulative update. As a result, any fax modem hardware dependent on this driver will no longer function on Windows. Microsoft advises organizations to eliminate any reliance on this hardware.

#3

Another actively exploited flaw, CVE-2025-59230, involves improper access control in Windows Remote Access Connection Manager, enabling an authorized attacker to elevate privileges locally and gain SYSTEM-level access. Similarly, CVE-2025-47827, a flaw in IGEL OS versions prior to 11, allows Secure Boot bypass due to improper verification of cryptographic signatures in the igel-flash-driver module. This could enable mounting a crafted root filesystem from an unverified SquashFS image.

#4

Several critical vulnerabilities also demand attention. CVE-2025-59246 in Azure Entra ID allows privilege escalation, while CVE-2025-59287 in Windows Server Update Service (WSUS) enables an unauthorized attacker to execute code remotely via deserialization of untrusted data. Another publicly disclosed critical flaw, CVE-2025-0033, impacts AMD EPYC processors using Secure Encrypted Virtualization – Secure Nested Paging (SEV-SNP). A race condition during Reverse Map Table (RMP) initialization could allow a malicious or compromised hypervisor to modify RMP entries before they are locked, potentially compromising SEV-SNP guest memory integrity. While this flaw does not expose plaintext data, it requires privileged hypervisor control to exploit. It is partially patched; a few product patches will be rolled out in the following months

#5 Other publicly disclosed vulnerabilities include CVE-2025-2884, affecting the TCG TPM 2.0 Reference Implementation. The CryptHmacSign helper function is vulnerable to out-of-bounds reads due to inadequate validation of the signature scheme against the key's algorithm. Additionally, CVE-2025-59489 impacts the Unity Gaming Engine Editor across Android, Windows, macOS, and Linux, allowing argument injection that could lead to loading library code from unintended locations. Applications built with affected Unity Editor versions could be exploited to execute code and exfiltrate sensitive information from affected systems.

#6 With a broad range of critical vulnerabilities, including actively exploited flaws, this Patch Tuesday highlights the importance of immediate action. Organizations are strongly advised to deploy updates without delay, review system dependencies, and verify security configurations to prevent potential exploitation.

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-2025-24990, CVE-2025-59230, and CVE-2025-47827. 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-2025-24052	Windows Agere Modem Driver Elevation of Privilege Vulnerability	Agere Windows Modem Driver	Elevation of Privilege
CVE-2025-24990	Microsoft Windows Untrusted Pointer Dereference Vulnerability	Agere Windows Modem Driver	Elevation of Privilege
CVE-2025-25004	PowerShell Elevation of Privilege Vulnerability	Microsoft PowerShell	Elevation of Privilege
CVE-2025-47979	Microsoft Failover Cluster Information Disclosure Vulnerability	Windows Failover Cluster	Information Disclosure
CVE-2025-47989	Azure Connected Machine Agent Elevation of Privilege Vulnerability	Azure Connected Machine Agent	Elevation of Privilege
CVE-2025-48004	Microsoft Brokering File System Elevation of Privilege Vulnerability	Microsoft Brokering File System	Elevation of Privilege
CVE-2025-48813	Virtual Secure Mode Spoofing Vulnerability	Virtual Secure Mode	Spoofing
CVE-2025-49708	Microsoft Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2025-50152	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-50174	Windows Device Association Broker Service Elevation of Privilege Vulnerability	Windows Device Association Broker service	Elevation of Privilege
CVE-2025-50175	Windows Digital Media Elevation of Privilege Vulnerability	Windows Digital Media	Elevation of Privilege
CVE-2025-53139	Windows Hello Security Feature Bypass Vulnerability	Windows Hello	Security Feature Bypass
CVE-2025-53150	Windows Digital Media Elevation of Privilege Vulnerability	Windows Digital Media	Elevation of Privilege
CVE-2025-53717	Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability	Windows Virtualization-Based Security (VBS) Enclave	Elevation of Privilege
CVE-2025-53768	Xbox IStorageService Elevation of Privilege Vulnerability	Xbox	Elevation of Privilege
CVE-2025-53782	Microsoft Exchange Server Elevation of Privilege Vulnerability	Microsoft Exchange Server	Elevation of Privilege
CVE-2025-55240	Visual Studio Elevation of Privilege Vulnerability	Visual Studio	Elevation of Privilege
CVE-2025-55247	.NET Elevation of Privilege Vulnerability	.NET	Elevation of Privilege
CVE-2025-55248	.NET, .NET Framework, and Visual Studio Information Disclosure Vulnerability	.NET, .NET Framework, Visual Studio	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2025-55315	ASP.NET Security Feature Bypass Vulnerability	ASP.NET Core	Security Feature Bypass
CVE-2025-55320	Configuration Manager Elevation of Privilege Vulnerability	Microsoft Configuration Manager	Elevation of Privilege
CVE-2025-55321	Azure Monitor Log Analytics Spoofing Vulnerability	Azure Monitor	Spoofing
CVE-2025-55325	Windows Storage Management Provider Information Disclosure Vulnerability	Windows Storage Management Provider	Information Disclosure
CVE-2025-55326	Windows Connected Devices Platform Service (Cdpsvc) Remote Code Execution Vulnerability	Connected Devices Platform Service (Cdpsvc)	Remote Code Execution
CVE-2025-55328	Windows Hyper-V Elevation of Privilege Vulnerability	Windows Hyper-V	Elevation of Privilege
CVE-2025-55330	Windows BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2025-55331	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Windows PrintWorkflow UserSvc	Elevation of Privilege
CVE-2025-55332	Windows BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2025-55333	Windows BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2025-55334	Windows Kernel Security Feature Bypass Vulnerability	Windows Kernel	Security Feature Bypass
CVE-2025-55335	Windows NTFS Elevation of Privilege Vulnerability	Windows NTFS	Elevation of Privilege
CVE-2025-55336	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability	Windows Cloud Files Mini Filter Driver	Information Disclosure
CVE-2025-55337	Windows BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2025-55338	Windows BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2025-55339	Windows Network Driver Interface Specification Driver Elevation of Privilege Vulnerability	Windows NDIS	Elevation of Privilege
CVE-2025-55340	Windows Remote Desktop Protocol Security Feature Bypass	Windows Remote Desktop Protocol	Security Feature Bypass
CVE-2025-55676	Windows USB Video Class System Driver Information Disclosure Vulnerability	Windows USB Video Driver	Information Disclosure
CVE-2025-55677	Windows Device Association Broker Service Elevation of Privilege Vulnerability	Windows Device Association Broker service	Elevation of Privilege
CVE-2025-55678	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Windows DirectX	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-55679	Windows Kernel Information Disclosure Vulnerability	Windows Kernel	Information Disclosure
CVE-2025-55680	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver	Elevation of Privilege
CVE-2025-55681	Desktop Windows Manager Elevation of Privilege Vulnerability	Windows DWM	Elevation of Privilege
CVE-2025-55682	Windows BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2025-55683	Windows Kernel Information Disclosure Vulnerability	Windows Kernel	Information Disclosure
CVE-2025-55684	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Windows PrintWorkflow UserSvc	Elevation of Privilege
CVE-2025-55685	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Windows PrintWorkflow UserSvc	Elevation of Privilege
CVE-2025-55686	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Windows PrintWorkflow UserSvc	Elevation of Privilege
CVE-2025-55687	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	Windows Resilient File System (ReFS)	Elevation of Privilege
CVE-2025-55688	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Windows PrintWorkflow UserSvc	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-55689	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Windows PrintWorkflow UserSvc	Elevation of Privilege
CVE-2025-55690	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Windows PrintWorkflow UserSvc	Elevation of Privilege
CVE-2025-55691	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Windows PrintWorkflow UserSvc	Elevation of Privilege
CVE-2025-55692	Windows Error Reporting Service Elevation of Privilege Vulnerability	Windows Error Reporting	Elevation of Privilege
CVE-2025-55693	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2025-55694	Windows Error Reporting Service Elevation of Privilege Vulnerability	Windows Error Reporting	Elevation of Privilege
CVE-2025-55695	Windows WLAN AutoConfig Service Information Disclosure Vulnerability	Windows WLAN Auto Config Service	Information Disclosure
CVE-2025-55696	NtQueryInformation Token function (ntifs.h) Elevation of Privilege Vulnerability	NtQueryInformation Token function (ntifs.h)	Elevation of Privilege
CVE-2025-55697	Azure Local Elevation of Privilege Vulnerability	Azure	Elevation of Privilege
CVE-2025-55698	DirectX Graphics Kernel Denial of Service Vulnerability	Windows DirectX	Denial of Service

CVE	NAME	PRODUCT	IMPACT
CVE-2025-55699	Windows Kernel Information Disclosure Vulnerability	Windows Kernel	Information Disclosure
CVE-2025-55700	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-55701	Windows Authentication Elevation of Privilege Vulnerability	Microsoft Windows	Elevation of Privilege
CVE-2025-58714	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-58715	Windows Speech Runtime Elevation of Privilege Vulnerability	Microsoft Windows Speech	Elevation of Privilege
CVE-2025-58716	Windows Speech Runtime Elevation of Privilege Vulnerability	Microsoft Windows Speech	Elevation of Privilege
CVE-2025-58717	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-58718	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2025-58719	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Connected Devices Platform Service (Cdpsvc)	Elevation of Privilege
CVE-2025-58720	Windows Cryptographic Services Information Disclosure Vulnerability	Windows Cryptographic Services	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2025-58722	Microsoft DWM Core Library Elevation of Privilege Vulnerability	Windows DWM	Elevation of Privilege
CVE-2025-58724	Arc Enabled Servers - Azure Connected Machine Agent Elevation of Privilege Vulnerability	Azure Connected Machine Agent	Elevation of Privilege
CVE-2025-58725	Windows COM+ Event System Service Elevation of Privilege Vulnerability	Windows COM	Elevation of Privilege
CVE-2025-58726	Windows SMB Server Elevation of Privilege Vulnerability	Windows SMB Server	Elevation of Privilege
CVE-2025-58727	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Windows Connected Devices Platform Service	Elevation of Privilege
CVE-2025-58728	Windows Bluetooth Service Elevation of Privilege Vulnerability	Windows Bluetooth Service	Elevation of Privilege
CVE-2025-58729	Windows Local Session Manager (LSM) Denial of Service Vulnerability	Windows Local Session Manager (LSM)	Denial of Service
CVE-2025-58730	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution
CVE-2025-58731	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution
CVE-2025-58732	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-58733	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution
CVE-2025-58734	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution
CVE-2025-58735	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution
CVE-2025-58736	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution
CVE-2025-58737	Remote Desktop Protocol Remote Code Execution Vulnerability	Windows Remote Desktop	Remote Code Execution
CVE-2025-58738	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution
CVE-2025-58739	Microsoft Windows File Explorer Spoofing Vulnerability	Windows File Explorer	Spoofing
CVE-2025-59184	Storage Spaces Direct Information Disclosure Vulnerability	Windows High Availability Services	Information Disclosure
CVE-2025-59185	NTLM Hash Disclosure Spoofing Vulnerability	Windows Core Shell	Spoofing
CVE-2025-59186	Windows Kernel Information Disclosure Vulnerability	Windows Kernel	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59187	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2025-59188	Microsoft Failover Cluster Information Disclosure Vulnerability	Windows Failover Cluster	Information Disclosure
CVE-2025-59189	Microsoft Brokering File System Elevation of Privilege Vulnerability	Microsoft Brokering File System	Elevation of Privilege
CVE-2025-59190	Windows Search Service Denial of Service Vulnerability	Microsoft Windows Search Component	Denial of Service
CVE-2025-59191	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Connected Devices Platform Service (Cdpsvc)	Elevation of Privilege
CVE-2025-59192	Storport.sys Driver Elevation of Privilege Vulnerability	Storport.sys Driver	Elevation of Privilege
CVE-2025-59193	Windows Management Services Elevation of Privilege Vulnerability	Windows Management Services	Elevation of Privilege
CVE-2025-59194	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2025-59195	Microsoft Graphics Component Denial of Service Vulnerability	Microsoft Graphics Component	Denial of Service
CVE-2025-59196	Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability	Windows SSDP Service	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59197	Windows ETL Channel Information Disclosure Vulnerability	Windows ETL Channel	Information Disclosure
CVE-2025-59198	Windows Search Service Denial of Service Vulnerability	Microsoft Windows Search Component	Denial of Service
CVE-2025-59199	Software Protection Platform (SPP) Elevation of Privilege Vulnerability	Software Protection Platform (SPP)	Elevation of Privilege
CVE-2025-59200	Data Sharing Service Spoofing Vulnerability	Data Sharing Service Client	Spoofing
CVE-2025-59201	Network Connection Status Indicator (NCSI) Elevation of Privilege Vulnerability	Network Connection Status Indicator (NCSI)	Elevation of Privilege
CVE-2025-59202	Windows Remote Desktop Services Elevation of Privilege Vulnerability	Windows Remote Desktop Services	Elevation of Privilege
CVE-2025-59203	Windows State Repository API Server File Information Disclosure Vulnerability	Windows StateRepository API	Information Disclosure
CVE-2025-59204	Windows Management Services Information Disclosure Vulnerability	Windows Management Services	Information Disclosure
CVE-2025-59205	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2025-59206	Windows Resilient File System (ReFS) Deduplication Service Elevation of Privilege Vulnerability	Windows Resilient File System (ReFS) Deduplication Service	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59207	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2025-59208	Windows MapUrlToZone Information Disclosure Vulnerability	Windows MapUrlToZone	Information Disclosure
CVE-2025-59209	Windows Push Notification Information Disclosure Vulnerability	Windows Push Notification Core	Information Disclosure
CVE-2025-59210	Windows Resilient File System (ReFS) Deduplication Service Elevation of Privilege Vulnerability	Windows Resilient File System (ReFS) Deduplication Service	Elevation of Privilege
CVE-2025-59211	Windows Push Notification Information Disclosure Vulnerability	Windows Push Notification Core	Information Disclosure
CVE-2025-59213	Configuration Manager Elevation of Privilege Vulnerability	Microsoft Configuration Manager	Elevation of Privilege
CVE-2025-59214	Microsoft Windows File Explorer Spoofing Vulnerability	Windows File Explorer	Spoofing
CVE-2025-59218	Azure Entra ID Elevation of Privilege Vulnerability	Azure Entra ID	Elevation of Privilege
CVE-2025-59221	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2025-59222	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59223	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-59224	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-59225	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-59226	Microsoft Office Visio Remote Code Execution Vulnerability	Microsoft Office Visio	Remote Code Execution
CVE-2025-59227	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-59228	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2025-59229	Microsoft Office Denial of Service Vulnerability	Microsoft Office	Denial of Service
CVE-2025-59230	Microsoft Windows Improper Access Control Vulnerability	Windows Remote Access Connection Manager	Elevation of Privilege
CVE-2025-59231	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-59232	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59233	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-59234	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-59235	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure
CVE-2025-59236	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-59237	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2025-59238	Microsoft PowerPoint Remote Code Execution Vulnerability	Microsoft Office PowerPoint	Remote Code Execution
CVE-2025-59241	Windows Health and Optimized Experiences Elevation of Privilege Vulnerability	Windows Health and Optimized Experiences Service	Elevation of Privilege
CVE-2025-59242	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-59243	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2025-59244	NTLM Hash Disclosure Spoofing Vulnerability	Windows Core Shell	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59246	Azure Entra ID Elevation of Privilege Vulnerability	Azure Entra ID	Elevation of Privilege
CVE-2025-59247	Azure PlayFab Elevation of Privilege Vulnerability	Azure PlayFab	Elevation of Privilege
CVE-2025-59248	Microsoft Exchange Server Spoofing Vulnerability	Microsoft Exchange Server	Spoofing
CVE-2025-59249	Microsoft Exchange Server Elevation of Privilege Vulnerability	Microsoft Exchange Server	Elevation of Privilege
CVE-2025-59250	JDBC Driver for SQL Server Spoofing Vulnerability	JDBC Driver for SQL Server	Spoofing
CVE-2025-59252	M365 Copilot Spoofing Vulnerability	Copilot	Spoofing
CVE-2025-59253	Windows Search Service Denial of Service Vulnerability	Microsoft Windows Search Component	Denial of Service
CVE-2025-59254	Microsoft DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2025-59255	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2025-59257	Windows Local Session Manager (LSM) Denial of Service Vulnerability	Windows Local Session Manager (LSM)	Denial of Service

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59258	Windows Active Directory Federation Services (ADFS) Information Disclosure Vulnerability	Active Directory Federation Services	Information Disclosure
CVE-2025-59259	Windows Local Session Manager (LSM) Denial of Service Vulnerability	Windows Local Session Manager (LSM)	Denial of Service
CVE-2025-59260	Microsoft Failover Cluster Virtual Driver Information Disclosure Vulnerability	Microsoft Failover Cluster Virtual Driver	Information Disclosure
CVE-2025-59261	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Graphics Component	Elevation of Privilege
CVE-2025-59271	Redis Enterprise Elevation of Privilege Vulnerability	Redis Enterprise	Elevation of Privilege
CVE-2025-59272	Copilot Spoofing Vulnerability	Copilot	Spoofing
CVE-2025-59275	Windows Authentication Elevation of Privilege Vulnerability	Windows Authentication Methods	Elevation of Privilege
CVE-2025-59277	Windows Authentication Elevation of Privilege Vulnerability	Windows Authentication Methods	Elevation of Privilege
CVE-2025-59278	Windows Authentication Elevation of Privilege Vulnerability	Windows Authentication Methods	Elevation of Privilege
CVE-2025-59280	Windows SMB Client Tampering Vulnerability	Windows SMB Client	Tampering

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59281	Xbox Gaming Services Elevation of Privilege Vulnerability	XBox Gaming Services	Elevation of Privilege
CVE-2025-59282	Internet Information Services (IIS) Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	Inbox COM Objects	Remote Code Execution
CVE-2025-59284	Windows NTLM Spoofing Vulnerability	Windows NTLM	Spoofing
CVE-2025-59285	Azure Monitor Agent Elevation of Privilege Vulnerability	Azure Monitor Agent	Elevation of Privilege
CVE-2025-59286	Copilot Spoofing Vulnerability	Copilot	Spoofing
CVE-2025-59287	Windows Server Update Service (WSUS) Remote Code Execution Vulnerability	Windows Server Update Service	Remote Code Execution
CVE-2025-59288	Playwright Spoofing Vulnerability	GitHub	Spoofing
CVE-2025-59289	Windows Bluetooth Service Elevation of Privilege Vulnerability	Windows Bluetooth Service	Elevation of Privilege
CVE-2025-59290	Windows Bluetooth Service Elevation of Privilege Vulnerability	Windows Bluetooth Service	Elevation of Privilege
CVE-2025-59291	Confidential Azure Container Instances Elevation of Privilege Vulnerability	Confidential Azure Container Instances	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-59292	Azure Compute Gallery Elevation of Privilege Vulnerability	Confidential Azure Container Instances	Elevation of Privilege
CVE-2025-59294	Windows Taskbar Live Preview Information Disclosure Vulnerability	Windows Taskbar Live	Information Disclosure
CVE-2025-59295	Windows URL Parsing Remote Code Execution Vulnerability	Internet Explorer	Remote Code Execution
CVE-2025-59494	Azure Monitor Agent Elevation of Privilege Vulnerability	Azure Monitor Agent	Elevation of Privilege
CVE-2025-59497	Microsoft Defender for Linux Denial of Service Vulnerability	Microsoft Defender for Linux	Denial of Service
CVE-2025-59502	Remote Procedure Call Denial of Service Vulnerability	Windows Remote Procedure Call	Denial of Service
CVE-2016-9535	LibTIFF Heap Buffer Overflow Vulnerability	Microsoft Graphics Component	Remote Code Execution
CVE-2025-0033	AMD Improper Access Control Vulnerability	AMD Restricted Memory Page	Remote Code Execution
CVE-2025-11205	Microsoft Edge WebGPU Heap Buffer Overflow Vulnerability	Microsoft Edge (Chromium-based)	Heap Buffer Overflow
CVE-2025-11206	Microsoft Edge Video Heap Buffer Overflow Vulnerability	Microsoft Edge (Chromium-based)	Heap Buffer Overflow

CVE	NAME	PRODUCT	IMPACT
CVE-2025-11207	Microsoft Edge Storage Side-Channel Information Leakage Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2025-11208	Microsoft Edge Media Inappropriate Implementation Vulnerability	Microsoft Edge (Chromium-based)	Affect Chrome's Handling of Media Content
CVE-2025-11209	Microsoft Edge Omnibox Inappropriate Implementation Vulnerability	Microsoft Edge (Chromium-based)	-
CVE-2025-11210	Microsoft Edge Tab Side-channel Information Leakage Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2025-11211	Microsoft Edge Media Out of Bounds Read Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure or System Crashes
CVE-2025-11212	Microsoft Edge Media Inappropriate Implementation Vulnerability	Microsoft Edge (Chromium-based)	Affect the Browser's Media Handling Capabilities
CVE-2025-11213	Microsoft Edge Omnibox Inappropriate Implementation Vulnerability	Microsoft Edge (Chromium-based)	Affect Chrome's Address Bar Functionality
CVE-2025-11215	Microsoft Edge V8 JavaScript Engine Off by One Error Vulnerability	Microsoft Edge (Chromium-based)	Memory Corruption
CVE-2025-11216	Microsoft Edge Storage Inappropriate Implementation Vulnerability	Microsoft Edge (Chromium-based)	-
CVE-2025-11219	Microsoft Edge V8 JavaScript Engine Use After Free Vulnerability	Microsoft Edge (Chromium-based)	Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-11458	Microsoft Edge Sync Heap Buffer Overflow Vulnerability	Microsoft Edge (Chromium-based)	Execution Of Arbitrary Code, Denial Of Service, or Information Disclosure
CVE-2025-11460	Microsoft Edge Storage Use After Free Vulnerability	Microsoft Edge (Chromium-based)	Execution Of Arbitrary Code, Denial Of Service, or Information Disclosure
CVE-2025-2884	TCG TPM2.0 Reference Implementation Out-of-Bounds Read Vulnerability	TCG TPM2.0	Information Disclosure
CVE-2025-47827	IGEL OS Use of a Key Past its Expiration Date Vulnerability	Windows Secure Boot	Security Feature Bypass
CVE-2025-54132	Mermaid Diagram Tool Arbitrary Image Fetch Vulnerability	Visual Studio	Information Disclosure
CVE-2025-54957	Dolby Digital Plus Audio Decoder Integer Overflow Vulnerability	Microsoft Windows Codecs Library	Remote Code Execution
CVE-2025-59489	Unity Gaming Engine Editor Vulnerability	Unity Gaming Engine Editor	Elevation of Privilege

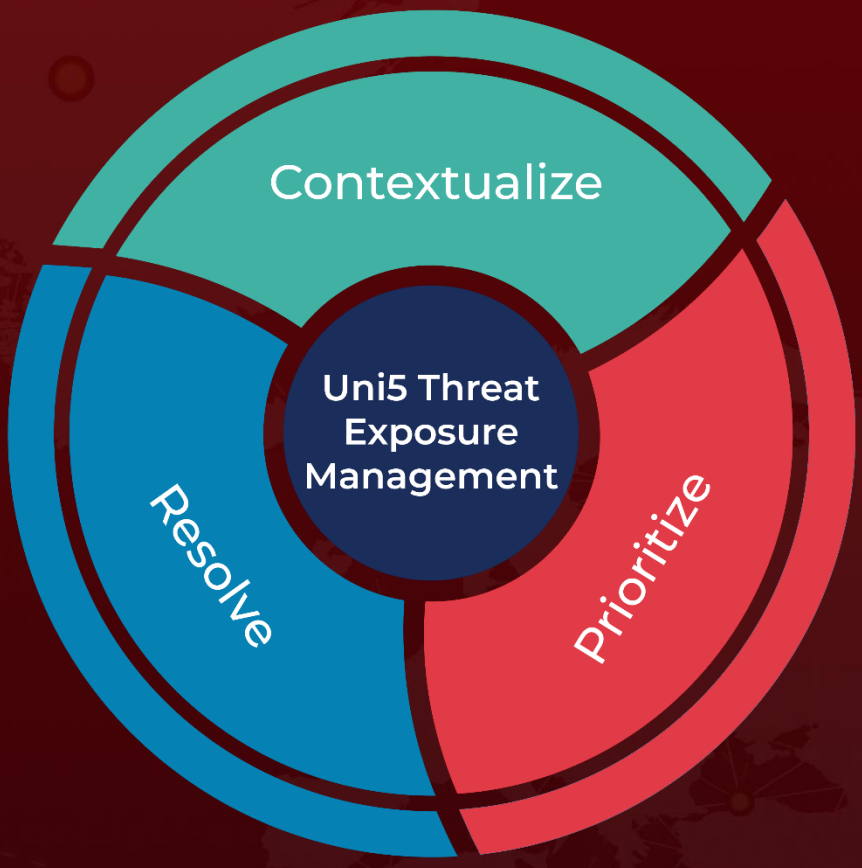
References

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

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

October 16, 2025 . 7:00 AM

More at www.hivepro.com