Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's July 2025 Patch Tuesday Fixes Active Zero-Day Exploits

Date of Publication	Last Update Date	Admiralty Code	TA Number
July 9, 2025	July 25, 2025	A1	TA2025210

Summary

First Seen: July 9, 2025
Affected Platforms: Microsoft SQL Server, Windows Kerberos, 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-2025-6554	Google Chromium V8 Type Confusion Vulnerability	Google Chromium, Microsoft Edge	✓	✓	✓
CVE-2025-6558	Google Chromium ANGLE and GPU Improper Input Validation Vulnerability	Google Chrome, Microsoft Edge	✓	✓	✓
CVE-2025-53770	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, and Microsoft SharePoint Server Subscription Edition	✓	✓	✓
CVE-2025-53771	Microsoft SharePoint Server Spoofing Vulnerability		✗	✗	✓
CVE-2025-49706	Microsoft SharePoint Improper Authentication Vulnerability		✗	✓	✓
CVE-2025-49704	Microsoft SharePoint Code Injection Vulnerability	Microsoft SharePoint Enterprise Server: 2016 - 2019	✗	✓	✓
CVE-2025-49719	Microsoft SQL Server Information Disclosure Vulnerability	Microsoft SQL Server: 2016 - 2022	✗	✗	✓
CVE-2025-47978	Windows Kerberos Denial of Service Vulnerability	Windows Server: 2022, 2025	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-47981	SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Remote Code Execution Vulnerability	Windows: 10 Windows Server: 2008 - 2016	✗	✗	✓
CVE-2025-47987	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	✗	✗	✓
CVE-2025-48001	BitLocker Security Feature Bypass Vulnerability	Windows: 10 Windows Server: 2012 - 2022	✗	✗	✓
CVE-2025-48799	Windows Update Service Elevation of Privilege Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2025	✗	✗	✓
CVE-2025-48800	BitLocker Security Feature Bypass Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	✗	✗	✓
CVE-2025-48804	BitLocker Security Feature Bypass Vulnerability	Windows: 10 Windows Server: 2012, 2016	✗	✗	✓
CVE-2025-48818	BitLocker Security Feature Bypass Vulnerability	Windows: 10 - 11 24H2 Windows Server – 2022, 2025	✗	✗	✓
CVE-2025-49695	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office LTSC: 2021- 2024 Microsoft Office LTSC for Mac: 2021 - 2024 Microsoft 365 Apps Microsoft Office: 2016 - 2019	✗	✗	✓
CVE-2025-49696	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office LTSC 2021 - 2024 Microsoft Office 2016 - 2019 Microsoft Office LTSC for Mac 2021 - 2024 Microsoft 365 Apps	✗	✗	✓
CVE-2025-49701	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint Enterprise Server: 2016 - 2019	✗	✗	✓

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

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-49704	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint Enterprise Server: 2016 - 2019	✗	✗	✓
CVE-2025-49718	Microsoft SQL Server Information Disclosure Vulnerability	Microsoft SQL Server 2019 - 2022	✗	✗	✓
CVE-2025-49724	Windows Connected Devices Platform Service Remote Code Execution Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2022, 2025	✗	✗	✓
CVE-2025-49727	Win32k Elevation of Privilege Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	✗	✗	✓
CVE-2025-49735	Windows KDC Proxy Service (KPSSVC) Remote Code Execution Vulnerability	Windows Server: 2012 - 2025	✗	✗	✓
CVE-2025-49744	Windows Graphics Component Elevation of Privilege Vulnerability	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	✗	✗	✓

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	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
TA0040 Impact	T1070 Indicator Removal	T1204 User Execution	T1189 Drive-by Compromise
T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1068 Exploitation for Privilege Escalation
T1588 Obtain Capabilities	T1588.005 Exploits	T1588.006 Vulnerabilities	T1498 Network Denial of Service
T1190 Exploit Public-Facing Application	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1505.003 Web Shell
T1552.001 Credentials In Files	T1083 File and Directory Discovery	T1018 Remote System Discovery	T1021.002 SMB/Windows Admin Shares
T1071.001 Web Protocols	T1033 System Owner/User Discovery	T1505 Server Software Component	T1569 System Services
T1569.002 Service Execution	T1543 Create or Modify System Process	T1543.003 Windows Service	T1047 Windows Management Instrumentation
T1505.004 IIS Components	T1053.005 Scheduled Task	T1484.001 Group Policy Modification	T1620 Reflective Code Loading
T1562.001 Disable or Modify Tools	T1112 Modify Registry	T1003.001 LSASS Memory	T1570 Lateral Tool Transfer
T1119 Automated Collection	T1005 Data from Local System	T1090 Proxy	T1486 Data Encrypted for Impact

Vulnerability Details

#1

Microsoft's July 2025 Patch Tuesday delivers an extensive batch of security updates, addressing 137 vulnerabilities across its product ecosystem. These include 18 rated critical, 118 marked important, and one moderate in severity. The vulnerabilities span various categories: 43 involve Remote Code Execution (RCE), 58 Elevation of Privilege, 17 Information Disclosure, 5 Denial of Service, 8 Security Feature Bypass, 5 Spoofing, and 1 Tampering issue. Beyond its own products, Microsoft also released patches for 13 non-Microsoft CVEs, pushing the total count of vulnerabilities addressed this month to 150. Notably, 24 of these CVEs are considered at risk of active exploitation, underscoring the urgency of prompt patch deployment.

#2

Among the standout flaws is CVE-2025-49719, an information disclosure vulnerability in Microsoft SQL Server. This issue allows an unauthorized attacker to access uninitialized memory content over a network, potentially exposing sensitive data. It has been publicly disclosed, making it a heightened concern for enterprise environments. Another major risk is CVE-2025-6554, a type confusion vulnerability in the V8 JavaScript engine used by Google Chrome. Affecting versions prior to 138.0.7204.96, this flaw was actively exploited in the wild before a fix became available, classifying it as a zero-day vulnerability.

#3

Two high-impact zero-day vulnerabilities, one in Google Chrome and another in Microsoft SharePoint Server are currently being exploited in the wild. CVE-2025-6558, a zero-day flaw in Chrome's graphics components, stems from weak input validation that allows attackers to escape the browser's sandbox simply by luring victims to a malicious HTML page.

#4

Meanwhile, CVE-2025-53770 targets Microsoft SharePoint Servers through unsafe deserialization of untrusted data, enabling unauthenticated remote code execution. This vulnerability, a variant of the CVE-2025-49706 spoofing flaw, is part of a broader exploit chain known as ToolShell. A related issue, CVE-2025-53771, allows directory traversal attacks that can be used for network-wide spoofing by authenticated users. These vulnerabilities alongside CVE-2025-49704 and CVE-2025-49706 can be chained for full system compromise. Nation-state actors like Linen Typhoon (APT27) and Violet Typhoon (APT31, JUDGMENT PANDA) have been observed exploiting these flaws for espionage. Additionally, Storm-2603 a threat actor linked to China has leveraged the same vulnerabilities for financially driven ransomware attacks.

#5

CVE-2025-49735 is another critical issue, involving a Remote Code Execution vulnerability in the Windows Key Distribution Center (KDC) Proxy Service. An unauthenticated attacker could exploit a weakness in its cryptographic protocol using a specially crafted application to gain remote code execution privileges on targeted systems.

#6

Microsoft Office received fixes for two critical local code execution vulnerabilities. CVE-2025-49695, a use-after-free flaw, and CVE-2025-49696, an out-of-bounds read issue, both allow attackers to execute code locally by manipulating Office files. These flaws, if weaponized through phishing or document-based attacks, could pose serious threats in enterprise environments. In a similar vein, Microsoft SharePoint Server was affected by CVE-2025-49704, an RCE vulnerability caused by improper code generation. An authenticated attacker could exploit this to execute arbitrary code remotely across the network.

#7

Additional patches address vulnerabilities in Windows security infrastructure. CVE-2025-47978, an out-of-bounds read in Windows Kerberos, could allow an authorized attacker to trigger a Denial of Service remotely. Another vulnerability, CVE-2025-47981, is a heap-based buffer overflow in SPNEGO Extended Negotiation, which could enable an unauthorized remote attacker to execute code. Several flaws were also resolved in BitLocker, including CVE-2025-48001, CVE-2025-48800, CVE-2025-48804, and CVE-2025-48818. SharePoint also saw additional coverage with CVE-2025-49701, further mitigating risk to collaborative platforms.

#8

Microsoft's July 2025 security update serves as a crucial reminder of the evolving threat landscape. Organizations are strongly encouraged to apply these patches without delay to reduce their attack surface and defend against both opportunistic and targeted threats.

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-2025-6554, CVE-2025-6558, CVE-2025-53770, CVE-2025-53771, CVE-2025-49706, CVE-2025-49704. 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-2025-6554	Google Chromium V8 Type Confusion Vulnerability	Google Chromium, Microsoft Edge	Arbitrary Read/Write
CVE-2025-49719	Microsoft SQL Server Information Disclosure Vulnerability	Microsoft SQL Server	Information Disclosure
CVE-2025-47978	Windows Kerberos Denial of Service Vulnerability	Windows Kerberos	Denial of Service
CVE-2025-47981	SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Remote Code Execution Vulnerability	Windows SPNEGO Extended Negotiation (NEGOEX)	Remote Code Execution
CVE-2025-47987	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability	Windows Credential Security Support Provider Protocol (CredSSP)	Elevation of Privilege
CVE-2025-48001	BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2025-48799	Windows Update Service Elevation of Privilege Vulnerability	Windows Update Service	Elevation of Privilege
CVE-2025-48800	BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2025-48804	BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2025-48818	BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	Security Feature Bypass
CVE-2025-49695	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-49696	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-49701	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	Remote Code Execution
CVE-2025-49704	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	Remote Code Execution
CVE-2025-49718	Microsoft SQL Server Information Disclosure Vulnerability	Microsoft SQL Server	Information Disclosure
CVE-2025-49724	Windows Connected Devices Platform Service Remote Code Execution Vulnerability	Windows Connected Devices Platform Service	Remote Code Execution
CVE-2025-49727	Win32k Elevation of Privilege Vulnerability	Windows Win32K	Elevation of Privilege
CVE-2025-49735	Windows KDC Proxy Service (KPSSVC) Remote Code Execution Vulnerability	Windows KDC Proxy Service (KPSSVC)	Remote Code Execution
CVE-2025-49744	Windows Graphics Component Elevation of Privilege Vulnerability	Windows Graphics Component	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-21195	Azure Service Fabric Runtime Elevation of Privilege Vulnerability	Azure Service Fabric Runtime	Elevation of Privilege
CVE-2025-26636	Windows Kernel Information Disclosure Vulnerability	Windows Kernel	Information Disclosure
CVE-2025-33054	Remote Desktop Spoofing Vulnerability	Remote Desktop Client	Spoofing
CVE-2025-47159	Windows Virtualization-Based Security (VBS) Elevation of Privilege Vulnerability	Windows Virtualization-Based Security (VBS)	Elevation of Privilege
CVE-2025-47178	Microsoft Configuration Manager Remote Code Execution Vulnerability	Microsoft Configuration Manager	Remote Code Execution
CVE-2025-47971	Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability	Microsoft Virtual Hard Disk	Elevation of Privilege
CVE-2025-47972	Windows Input Method Editor (IME) Elevation of Privilege Vulnerability	Windows Input Method Editor (IME)	Elevation of Privilege
CVE-2025-47973	Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability	Microsoft Virtual Hard Disk	Elevation of Privilege
CVE-2025-47975	Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability	Windows Simple Search and Discovery Protocol (SSDP) Service	Elevation of Privilege
CVE-2025-47976	Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability	Windows Simple Search and Discovery Protocol (SSDP) Service	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-47980	Windows Imaging Component Information Disclosure Vulnerability	Windows Imaging Component	Information Disclosure
CVE-2025-47982	Windows Storage VSP Driver Elevation of Privilege Vulnerability	Windows Storage VSP Driver	Elevation of Privilege
CVE-2025-47984	Windows GDI Information Disclosure Vulnerability	Windows GDI	Information Disclosure
CVE-2025-47985	Windows Event Tracing Elevation of Privilege Vulnerability	Windows Event Tracing	Elevation of Privilege
CVE-2025-47986	Universal Print Management Service Elevation of Privilege Vulnerability	Universal Print Management Service	Elevation of Privilege
CVE-2025-47988	Remote Code Execution Vulnerability	Azure Monitor Agent	Remote Code Execution
CVE-2025-47991	Windows Input Method Editor (IME) Elevation of Privilege Vulnerability	Windows Input Method Editor (IME)	Elevation of Privilege
CVE-2025-47993	Microsoft PC Manager Elevation of Privilege Vulnerability	Microsoft PC Manager	Elevation of Privilege
CVE-2025-47994	Microsoft Office Elevation of Privilege Vulnerability	Microsoft Office	Elevation of Privilege
CVE-2025-47996	Windows MBT Transport Driver Elevation of Privilege Vulnerability	Windows MBT Transport Driver	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-47998	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-47999	Windows Hyper-V Denial of Service Vulnerability	Windows Hyper-V	Denial of Service
CVE-2025-48000	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Windows Connected Devices Platform Service	Elevation of Privilege
CVE-2025-48002	Windows Hyper-V Information Disclosure Vulnerability	Windows Hyper-V	Information Disclosure
CVE-2025-48003	BitLocker Security Feature Bypass Vulnerability	BitLocker	Security Feature Bypass
CVE-2025-48802	Windows SMB Server Spoofing Vulnerability	Windows SMB Server	Spoofing
CVE-2025-48803	Windows Virtualization-Based Security (VBS) Elevation of Privilege Vulnerability	Windows Virtualization-Based Security (VBS)	Elevation of Privilege
CVE-2025-48805	Microsoft MPEG-2 Video Extension Remote Code Execution Vulnerability	Microsoft MPEG-2 Video Extension	Remote Code Execution
CVE-2025-48806	Microsoft MPEG-2 Video Extension Remote Code Execution Vulnerability	Microsoft MPEG-2 Video Extension	Remote Code Execution
CVE-2025-48808	Windows Kernel Information Disclosure Vulnerability	Windows Kernel	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2025-48809	Windows Secure Kernel Mode Information Disclosure Vulnerability	Windows Secure Kernel Mode	Information Disclosure
CVE-2025-48810	Windows Secure Kernel Mode Information Disclosure Vulnerability	Windows Secure Kernel Mode	Information Disclosure
CVE-2025-48811	Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability	Windows Virtualization-Based Security (VBS)	Elevation of Privilege
CVE-2025-48812	Microsoft Excel Information Disclosure Vulnerability	Microsoft Excel	Information Disclosure
CVE-2025-48814	Remote Desktop Licensing Service Security Feature Bypass Vulnerability	Remote Desktop Licensing Service	Security Feature Bypass
CVE-2025-48815	Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability	Windows Simple Search and Discovery Protocol (SSDP)	Elevation of Privilege
CVE-2025-48816	HID Class Driver Elevation of Privilege Vulnerability	HID Class Driver	Elevation of Privilege
CVE-2025-48817	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	Remote Code Execution
CVE-2025-48819	Windows Universal Plug and Play (UPnP) Device Host Elevation of Privilege Vulnerability	Windows Universal Plug and Play (UPnP) Device Host	Elevation of Privilege
CVE-2025-48820	Windows AppX Deployment Service Elevation of Privilege Vulnerability	Windows AppX Deployment Service	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-48821	Windows Universal Plug and Play (UPnP) Device Host Elevation of Privilege Vulnerability	Windows Universal Plug and Play (UPnP) Device Host	Elevation of Privilege
CVE-2025-48822	Windows Hyper-V Discrete Device Assignment (DDA) Remote Code Execution Vulnerability	Windows Hyper-V Discrete Device Assignment (DDA)	Remote Code Execution
CVE-2025-48823	Windows Cryptographic Services Information Disclosure Vulnerability	Windows Cryptographic Services	Information Disclosure
CVE-2025-48824	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49657	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49658	Windows Transport Driver Interface (TDI) Translation Driver Information Disclosure Vulnerability	Windows Transport Driver Interface (TDI)	Information Disclosure
CVE-2025-49659	Windows Transport Driver Interface (TDI) Translation Driver Elevation of Privilege Vulnerability	Windows Transport Driver Interface (TDI)	Elevation of Privilege
CVE-2025-49660	Windows Event Tracing Elevation of Privilege Vulnerability	Windows Event Tracing	Elevation of Privilege
CVE-2025-49661	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2025-49663	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-2025-49664	Windows User-Mode Driver Framework Host Information Disclosure Vulnerability	Windows User-Mode Driver Framework	Information Disclosure
CVE-2025-49665	Workspace Broker Elevation of Privilege Vulnerability	Workspace Broker	Elevation of Privilege
CVE-2025-49666	Windows Server Setup and Boot Event Collection Remote Code Execution Vulnerability	Windows Server Setup and Boot Event Collection	Remote Code Execution
CVE-2025-49667	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Windows Win32 Kernel Subsystem	Elevation of Privilege
CVE-2025-49668	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49669	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49670	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49671	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-49672	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49673	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-2025-49674	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49675	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Kernel Streaming WOW Thunk Service Driver	Elevation of Privilege
CVE-2025-49676	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49677	Microsoft Brokering File System Elevation of Privilege Vulnerability	Microsoft Brokering File System	Elevation of Privilege
CVE-2025-49678	NTFS Elevation of Privilege Vulnerability	NTFS	Elevation of Privilege
CVE-2025-49679	Windows Shell Elevation of Privilege Vulnerability	Windows Shell	Elevation of Privilege
CVE-2025-49680	Windows Performance Recorder (WPR) Denial of Service Vulnerability	Windows Performance Recorder (WPR)	Denial of Service
CVE-2025-49681	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Windows Routing and Remote Access Service (RRAS)	Information Disclosure
CVE-2025-49682	Windows Media Elevation of Privilege Vulnerability	Windows Media	Elevation of Privilege
CVE-2025-49683	Microsoft Virtual Hard Disk Remote Code Execution Vulnerability	Microsoft Virtual Hard Disk	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-49684	Windows Storage Port Driver Information Disclosure Vulnerability	Windows Storage Port Driver	Information Disclosure
CVE-2025-49685	Windows Search Service Elevation of Privilege Vulnerability	Windows Search Service	Elevation of Privilege
CVE-2025-49686	Windows TCP/IP Driver Elevation of Privilege Vulnerability	Windows TCP/IP Driver	Elevation of Privilege
CVE-2025-49687	Windows Input Method Editor (IME) Elevation of Privilege Vulnerability	Windows Input Method Editor (IME)	Elevation of Privilege
CVE-2025-49688	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49689	Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability	Microsoft Virtual Hard Disk	Elevation of Privilege
CVE-2025-49690	Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	Capability Access Management Service (camsvc)	Elevation of Privilege
CVE-2025-49691	Windows Miracast Wireless Display Remote Code Execution Vulnerability	Windows Miracast Wireless Display	Remote Code Execution
CVE-2025-49693	Microsoft Brokering File System Elevation of Privilege Vulnerability	Microsoft Brokering File System	Elevation of Privilege
CVE-2025-49694	Microsoft Brokering File System Elevation of Privilege Vulnerability	Microsoft Brokering File System	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-49697	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-49698	Microsoft Word Remote Code Execution Vulnerability	Microsoft Word	Remote Code Execution
CVE-2025-49699	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-49700	Microsoft Word Remote Code Execution Vulnerability	Microsoft Word	Remote Code Execution
CVE-2025-49702	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2025-49703	Microsoft Word Remote Code Execution Vulnerability	Microsoft Word	Remote Code Execution
CVE-2025-49705	Microsoft PowerPoint Remote Code Execution Vulnerability	Microsoft PowerPoint	Remote Code Execution
CVE-2025-49706	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft SharePoint Server	Spoofing
CVE-2025-49711	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Excel	Remote Code Execution
CVE-2025-49713	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	Microsoft Edge	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2025-49714	Visual Studio Code Python Extension Remote Code Execution Vulnerability	Visual Studio Code Python Extension	Remote Code Execution
CVE-2025-49716	Windows Netlogon Denial of Service Vulnerability	Windows Netlogon	Denial of Service
CVE-2025-49717	Microsoft SQL Server Remote Code Execution Vulnerability	Microsoft SQL Server	Remote Code Execution
CVE-2025-49721	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability	Windows Fast FAT File System Driver	Elevation of Privilege
CVE-2025-49722	Windows Print Spooler Denial of Service Vulnerability	Windows Print Spooler	Denial of Service
CVE-2025-49723	Windows StateRepository API Server file Tampering Vulnerability	Windows StateRepository API	Tampering
CVE-2025-49725	Windows Notification Elevation of Privilege Vulnerability	Windows Notification	Elevation of Privilege
CVE-2025-49726	Windows Notification Elevation of Privilege Vulnerability	Windows Notification	Elevation of Privilege
CVE-2025-49729	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution
CVE-2025-49730	Microsoft Windows QoS Scheduler Driver Elevation of Privilege Vulnerability	Microsoft Windows QoS Scheduler Driver	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2025-49731	Microsoft Teams Elevation of Privilege Vulnerability	Microsoft Teams	Elevation of Privilege
CVE-2025-49732	Windows Graphics Component Elevation of Privilege Vulnerability	Windows Graphics Component	Elevation of Privilege
CVE-2025-49733	Win32k Elevation of Privilege Vulnerability	Win32k	Elevation of Privilege
CVE-2025-49737	Microsoft Teams Elevation of Privilege Vulnerability	Microsoft Teams	Elevation of Privilege
CVE-2025-49738	Microsoft PC Manager Elevation of Privilege Vulnerability	Microsoft PC Manager	Elevation of Privilege
CVE-2025-49739	Visual Studio Elevation of Privilege Vulnerability	Visual Studio	Elevation of Privilege
CVE-2025-49740	Windows SmartScreen Security Feature Bypass Vulnerability	Windows SmartScreen	Security Feature Bypass
CVE-2025-49741	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2025-49742	Windows Graphics Component Remote Code Execution Vulnerability	Windows Graphics Component	Remote Code Execution
CVE-2025-49753	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-2025-49756	Office Developer Platform Security Feature Bypass Vulnerability	Office Developer Platform	Security Feature Bypass
CVE-2025-49760	Windows Storage Spoofing Vulnerability	Windows Storage	Spoofing
CVE-2025-27613	Gitk Arguments Vulnerability	Gitk	File Creation/Truncation
CVE-2025-27614	Gitk Arbitrary Code Execution Vulnerability	Gitk	Arbitrary Script Execution
CVE-2024-36350	AMD: Transient Scheduler Attack in Store Queue Vulnerability	AMD	Information Disclosure
CVE-2025-36357	AMD: Transient Scheduler Attack in L1 Data Queue Vulnerability	AMD	Information Disclosure
CVE-2025-46334	Git Malicious Shell Vulnerability	Git	Malicious Shell Execution
CVE-2025-46835	Git File Overwrite Vulnerability	Git	Arbitrary File Overwrite
CVE-2025-48384	Git Symlink Vulnerability	Git	Arbitrary File Write
CVE-2025-48385	Git Protocol Injection Vulnerability	Git	Bundle Protocol Injection, Arbitrary File Write, RCE
CVE-2025-48386	Git wincred Credential Helper Buffer Overflow Vulnerability	Git	Buffer Overflow

CVE	NAME	PRODUCT	IMPACT
CVE-2025-6558	Google Chromium ANGLE and GPU Improper Input Validation Vulnerability	Google Chromium, Microsoft Edge	Sandbox Escape
CVE-2025-7656	Google Chrome Integer overflow in V8 Vulnerability	Google Chrome, Microsoft Edge	Heap Corruption
CVE-2025-7657	Google Chrome Use after free in WebRTC Vulnerability	Google Chrome, Microsoft Edge	Heap Corruption
CVE-2025-47158	Azure DevOps Server Elevation of Privilege Vulnerability	Azure DevOps Server	Elevation of Privilege
CVE-2025-47995	Azure Machine Learning Elevation of Privilege Vulnerability	Azure	Elevation of Privilege
CVE-2025-49746	Azure Machine Learning Elevation of Privilege Vulnerability	Azure	Elevation of Privilege
CVE-2025-49747	Azure Machine Learning Elevation of Privilege Vulnerability	Azure	Elevation of Privilege
CVE-2025-53762	Microsoft Purview Elevation of Privilege Vulnerability	Microsoft Purview	Elevation of Privilege
CVE-2025-53770	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	Remote Code Execution
CVE-2025-53771	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft SharePoint Server	Spoofing

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	107[.]191[.]58[.]76, 96[.]9[.]125[.]147, 172[.]174[.]82[.]132, 103[.]186[.]30[.]186, 131[.]226[.]2[.]6, 134[.]199[.]202[.]205, 104[.]238[.]159[.]149, 188[.]130[.]206[.]168, 65[.]38[.]121[.]198,
HTTP POST URI	/_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx
HTTP Referer Header	/_layouts/SignOut.aspx
URLs	c34718cbb4c6[.]ngrok-free[.]app/file[.]ps1, msupdate[.]updatemicfosoft[.]com
SHA256	92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514, 4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030, b39c14becb62aeb55df7fd55c814afbb0d659687d947d917512fe67973100b70, fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7, 24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf, b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0, c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94, 1eb914c09c873f0a7bcf81475ab0f6bdfaccc6b63bf7e5f2dbf19295106af192, 4c1750a14915bf2c0b093c2cb59063912dfa039a2adfe6d26d6914804e2ae928, 83705c75731e1d590b08f9357bc3b0f04741e92a033618736387512b40dab060, f54ae00a9bae73da001c4d3d690d26ddf5e8e006b5562f936df472ec5e299441, b180ab0a5845ed619939154f67526d2b04d28713fcc1904fbd666275538f431d,

TYPE	VALUE
SHA256	6753b840cec65dfba0d7d326ec768bff2495784c60db6a139f51c5e83349ac4d, 7ae971e40528d364fa52f3bb5e0660ac25ef63e082e3bbd54f153e27b31eae68, 567cb8e8c8bd0d909870c656b292b57bcb24eb55a8582b884e0a228e298e7443, 445a37279d3a229ed18513e85f0c8d861c6f560e0f914a5869df14a74b679b86, ffbc9dfc284b147e07a430fe9471e66c716a84a1f18976474a54bee82605fa9a, 6b273c2179518dacb1218201fd37ee2492a5e1713be907e69bf7ea56ceca53a5, c2c1fec7856e8d49f5d49267e69993837575dbbec99cd702c5be134a85b2c139, 6f6db63ece791c6dc1054f1e1231b5bbcf6c051a49bad0784569271753e24619, d6da885c90a5d1fb88d0a3f0b5d9817a82d5772d5510a0773c80ca581ce2486d, 62881359e75c9e8899c4bc9f452ef9743e68ce467f8b3e4398bebacde9550dea
File Path	C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\spinstall0.aspx, C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\15\TEMPLATE\LAYOUTS\spinstall0.aspx, \1[5-6]\TEMPLATE\LAYOUTS\debug_dev.js
Filename	Spinstall0.aspx, IIS_Server_dll.dll, SharpHostInfo.x64.exe, xd.exe, debug_dev.js

References

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

https://hivepro.com/threat-advisory/cve-2025-6554-google-chromes-zero-day-flaw-exploited-in-the-wild/

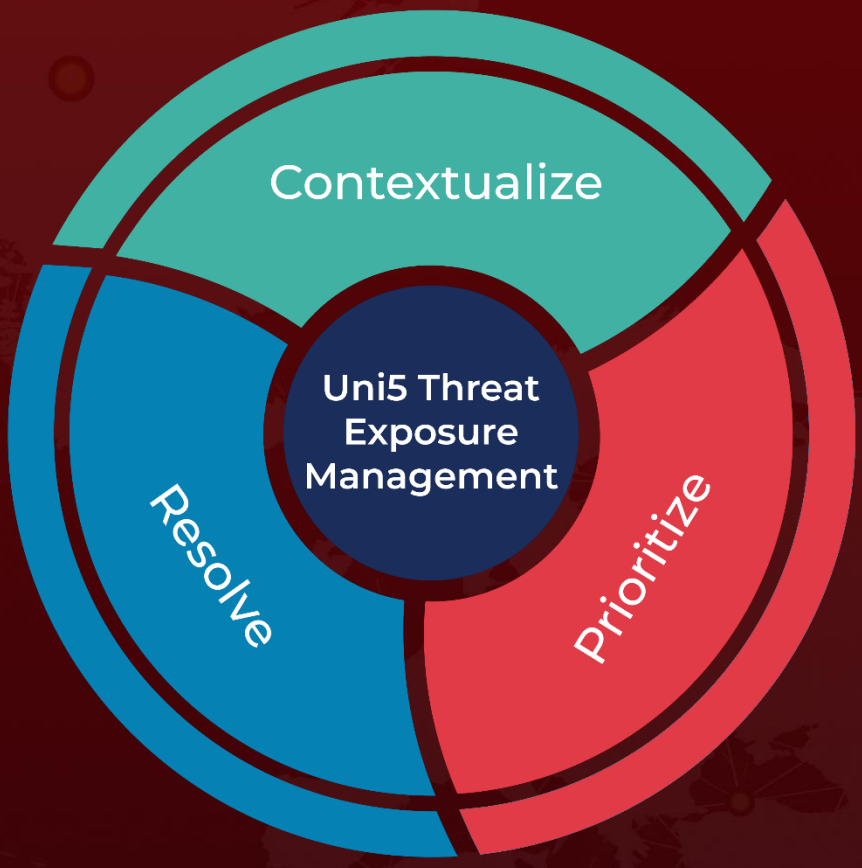
https://hivepro.com/threat-advisory/cve-2025-6558-chrome-flaw-lets-hackers-break-the-sandbox/

https://hivepro.com/threat-advisory/zero-day-watch-cve-2025-53770-turns-sharepoint-into-a-pivot-point/

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

July 9, 2025 . 8:50 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com