Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's July 2025 Patch Tuesday Addresses 130 Vulnerabilities

Date of Publication	Admiralty Code	TA Number
July 9, 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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-49719	Microsoft SQL Server Information Disclosure Vulnerability	Microsoft SQL Server	✗	✗	✓
CVE-2025-47978	Windows Kerberos Denial of Service Vulnerability	Windows Kerberos	✗	✗	✓
CVE-2025-47981	SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Remote Code Execution Vulnerability	Windows SPNEGO Extended Negotiation (NEGOEX)	✗	✗	✓
CVE-2025-47987	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability	Windows Credential Security Support Provider Protocol (CredSSP)	✗	✗	✓
CVE-2025-48001	BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-48799	Windows Update Service Elevation of Privilege Vulnerability	Windows Update Service	✗	✗	✓
CVE-2025-48800	BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	✗	✗	✓
CVE-2025-48804	BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	✗	✗	✓
CVE-2025-48818	BitLocker Security Feature Bypass Vulnerability	Windows BitLocker	✗	✗	✓
CVE-2025-49695	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	✗	✗	✓
CVE-2025-49696	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	✗	✗	✓
CVE-2025-49701	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✗	✓
CVE-2025-49704	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✗	✓
CVE-2025-49718	Microsoft SQL Server Information Disclosure Vulnerability	Microsoft SQL Server	✗	✗	✓
CVE-2025-49724	Windows Connected Devices Platform Service Remote Code Execution Vulnerability	Windows Connected Devices Platform Service	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-49727	Win32k Elevation of Privilege Vulnerability	Windows Win32K	✗	✗	✓
CVE-2025-49735	Windows KDC Proxy Service (KPSSVC) Remote Code Execution Vulnerability	Windows KDC Proxy Service (KPSSVC)	✗	✗	✓
CVE-2025-49744	Windows Graphics Component Elevation of Privilege Vulnerability	Windows Graphics Component	✗	✗	✓
CVE-2025-6554	Google Chromium V8 Type Confusion Vulnerability	Google Chromium	✓	✓	✓

Vulnerability Details

#1

Microsoft's July 2025 Patch Tuesday delivers an extensive batch of security updates, addressing 130 vulnerabilities across its product ecosystem. These include 12 rated critical, 117 marked important, and one moderate in severity. The vulnerabilities span various categories: 42 involve Remote Code Execution (RCE), 53 Elevation of Privilege, 17 Information Disclosure, 5 Denial of Service, 8 Security Feature Bypass, 4 Spoofing, and 1 Tampering issue. Beyond its own products, Microsoft also released patches for 10 non-Microsoft CVEs, pushing the total count of vulnerabilities addressed this month to 140. Notably, 19 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

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.

#4

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.

#5

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.

#6

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.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-49719	Microsoft SQL Server: 2016 - 2022	cpe:2.3:a:microsoft:sql_server:*:*:*:*:*:*:*:*	CWE-20
CVE-2025-47978	Windows Server: 2022 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-125
CVE-2025-47981	Windows: 10 Windows Server: 2008 - 2016	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-47987	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122 CWE-190
CVE-2025-48001	Windows: 10 Windows Server: 2012 - 2022	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-367
CVE-2025-48799	Windows: 10 - 11 24H2 Windows Server: 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-59
CVE-2025-48800	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-693

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-48804	Windows: 10 Windows Server: 2012 - 2016	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-349
CVE-2025-48818	Windows: 10 - 11 24H2 Windows Server - 2022 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-367
CVE-2025-49695	Microsoft Office LTSC: 2021-2024 Microsoft Office LTSC for Mac: 2021 - 2024 Microsoft 365 Apps Microsoft Office: 2016 - 2019	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-49696	Microsoft Office LTSC 2021 - 2024 Microsoft Office 2016 - 2019 Microsoft Office LTSC for Mac 2021 - 2024 Microsoft 365 Apps	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365:*:*:*:*:*:*:*:*	CWE-125 CWE-122
CVE-2025-49701	Microsoft SharePoint Enterprise Server: 2016 - 2019	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*:*:*	CWE-285
CVE-2025-49704	Microsoft SharePoint Enterprise Server: 2016 - 2019	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*:*:*	CWE-94
CVE-2025-49718	Microsoft SQL Server 2019 - 2022	cpe:2.3:a:microsoft:sql_server:*:*:*:*:*:*:*:*	CWE-908
CVE-2025-49724	Windows: 10 - 11 24H2 Windows Server: 2022 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-49727	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-122

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-49735	Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-49744	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122 CWE-191 CWE-362
CVE-2025-6554	Google Chrome prior to 138.0.7204.96	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-843

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 vulnerability CVE-2025-6554. This vulnerability 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.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0005 Defense Evasion	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			

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49719

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-47978

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-47981

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-47987

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-48001

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-48799

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-48800

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-48804

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-48818

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49695

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49696

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49701

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49704

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49718

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49724

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49727

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49735

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49744

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-6554

References

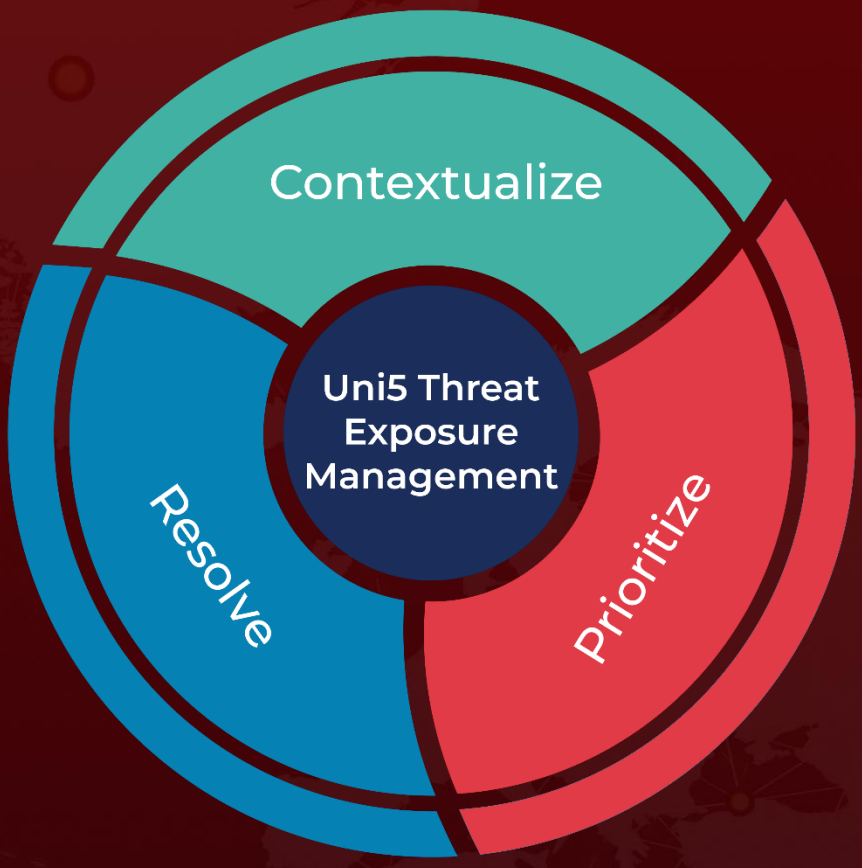
https://msrc.microsoft.com/update-guide/releaseNote/2025-Jul

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

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

More at www.hivepro.com