Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

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

Date of Publication	Admiralty Code	TA Number
March 13, 2025	A1	TA2025076

Summary

First Seen: March 11, 2025
Affected Platforms: Microsoft Windows, Microsoft Office, Windows Kernel, Windows Remote Desktop Services, Windows NTFS, Microsoft Management Console, and more.
Impact: Denial of Service (DoS), Elevation of Privilege (EoP), Remote Code Execution (RCE), Information Disclosure, Security Feature Bypass and Spoofing.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-24983	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-24984	Windows NTFS Information Disclosure Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-24985	Windows Fast FAT File System Driver Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-24991	Windows NTFS Information Disclosure Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-24993	Windows NTFS Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-26633	Microsoft Management Console Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-26630	Microsoft Access Remote Code Execution Vulnerability	Microsoft Access	✗	✗	✓
CVE-2025-24061	Windows Mark of the Web Security Feature Bypass Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-24066	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-24067	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-24992	Windows NTFS Information Disclosure Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-24995	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-9157	Synaptics Service Binaries DLL Loading Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21180	Windows exFAT File System Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21247	MapUrlToZone Security Feature Bypass Vulnerability	Microsoft Windows MapUrlToZone	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-24035	Windows Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-24044	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-24045	Windows Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓

Vulnerability Details

#1

Microsoft's March 2025 Patch Tuesday includes security updates for 57 vulnerabilities, classified as 6 critical, 50 important, and 1 moderate-severity vulnerability. These encompass 23 Remote Code Execution, 22 Elevation of Privilege, 4 Information Disclosure, 1 Denial of Service, 3 Security Feature Bypass, and 4 Spoofing vulnerabilities. The updates apply to a broad range of Microsoft products, including Windows, Office, Visual Studio, Windows Remote Desktop Services, Windows Hyper-V, Microsoft Management Console, and other components.

#2

Notably, Microsoft also patched ten non-Microsoft vulnerabilities. This includes one assigned to Windows by Synaptics, and nine assigned by Chome affecting the Chromium-based Microsoft Edge browser, bringing the total number of CVEs to 67. This advisory addresses 18 CVEs with potential exploitation risks.

#3 The update resolves six zero-day vulnerabilities that are actively being exploited in the wild and one that has been publicly disclosed before a patch was available. This extensive patch cycle aims to address critical issues and enhance overall system security.

#4 Among the actively exploited zero-day vulnerabilities, CVE-2025-24983 is an elevation of privilege vulnerability in the Windows Win32 Kernel Subsystem, allowing attackers to gain SYSTEM privileges by exploiting a race condition. This vulnerability affects older supported Windows systems and requires attackers to have low privileges on the network.

#5 Another notable vulnerability is CVE-2025-24993, a critical remote code execution flaw in Windows NTFS. It allows attackers to run arbitrary code in kernel context by mounting a malicious VHD, posing a significant threat to Windows NTFS systems.

#6 Other vulnerabilities include CVE-2025-24984 and CVE-2025-24991, both of which are information disclosure vulnerabilities in Windows NTFS. These flaws enable attackers with physical access to read sensitive data via malicious USB drives or VHD mounting.

#7 Additionally, CVE-2025-24985 is a remote code execution vulnerability affecting the Windows Fast FAT File System Driver, which could allow attackers to execute arbitrary code on affected systems. Lastly, CVE-2025-26633 is a security feature bypass vulnerability in Microsoft Management Console, requiring user interaction to bypass security features.

#8 The publicly disclosed vulnerability is CVE-2025-26630, a remote code execution flaw in Microsoft Access caused by a use-after-free memory bug. Exploitation requires tricking users into opening a specially crafted Access file, typically through phishing or social engineering attacks.

#9 The update also addressed several critical vulnerabilities that, while not zero-days, pose significant risks. Notably, two critical remote code execution vulnerabilities in Windows Remote Desktop Services, CVE-2025-24035 and CVE-2025-24045, were also patched. Both involve sensitive data storage issues and allow unauthorized network-based attackers to execute code without user interaction across network-connected Windows systems. These vulnerabilities underscore the importance of applying the March 2025 patches to protect against potential exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24983	Windows: 10 Windows Server: 2008 - 2016	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-24984	Windows: 10 - 11 24H2 Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-532
CVE-2025-24985	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-190 CWE-122
CVE-2025-24991	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-125
CVE-2025-24993	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-26633	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-707
CVE-2025-26630	Microsoft Office 2019 Microsoft Access 2016 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:access:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:*	CWE-416

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24061	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-693
CVE-2025-24066	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-24067	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-24992	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-126
CVE-2025-24995	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2024-9157	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-284
CVE-2025-21180	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-21247	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-41

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24035	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-591
CVE-2025-24044	Windows: 10 - 11 24H2 Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-24045	Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-591

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-2025-24983, CVE-2025-24984, CVE-2025-24985, CVE-2025-24991, CVE-2025-24993, and CVE-2025-26633. 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.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	TA0042 Resource Development	TA0040 Impact	TA0002 Execution
TA0008 Lateral Movement	TA0001 Initial Access	TA0005 Defense Evasion	TA0006 Credential Access
T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1203 Exploitation for Client Execution
T1498 Network Denial of Service	T1566 Phishing	T1204 User Execution	T1210 Exploitation of Remote Services
T1133 External Remote Services	T1212 Exploitation for Credential Access	T1553.005 Mark-of-the-Web Bypass	T1553 Subvert Trust Controls
T1189 Drive-by Compromise	T1588 Obtain Capabilities	T1588.005 Exploits	

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26630

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24061

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24066

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24067

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24992

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24995

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9157

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21180

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21247

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24035

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24044

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24045

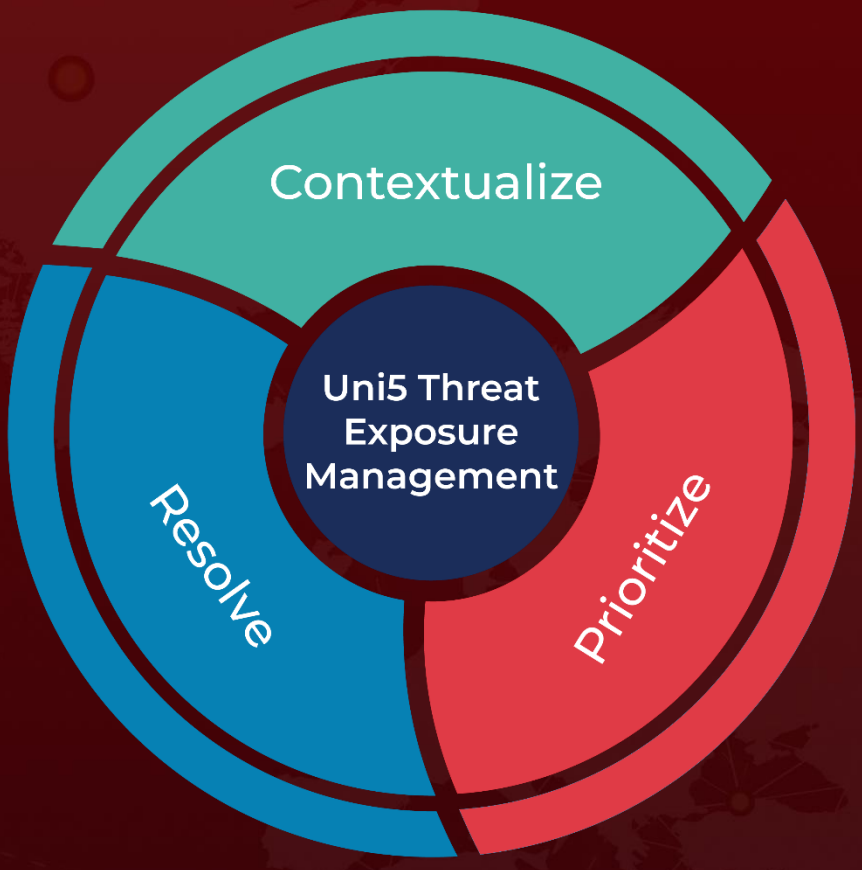
References

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

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

March 13, 2025 • 3:30 AM

More at www.hivepro.com