Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft Shuts Down Five Zero-Days in Latest Patch Rollout

Date of Publication	Admiralty Code	TA Number
May 15, 2025	A1	TA2025151

Summary

First Seen: May 13, 2025
Affected Products: Microsoft Windows, Visual Studio, Microsoft Office, Microsoft Office SharePoint, Windows Win32K, Windows Server
Impact: Elevation of Privilege (EoP), Remote Code Execution (RCE), Spoofing, Denial of Service

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-30400	Microsoft DWM Core Library Elevation of Privilege Vulnerability	Windows DWM	✓	✓	✓
CVE-2025-32701	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	✓	✓	✓
CVE-2025-32706	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	✓	✓	✓
CVE-2025-32709	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	✓	✓	✓
CVE-2025-30397	Scripting Engine Memory Corruption Vulnerability	Microsoft Scripting Engine	✓	✓	✓
CVE-2025-32702	Visual Studio Remote Code Execution Vulnerability	Visual Studio	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-30386	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	✗	✗	✓
CVE-2025-26685	Microsoft Defender for Identity Spoofing Vulnerability	Microsoft Defender for Identity	✗	✗	✓
CVE-2025-29967	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Gateway Service	✗	✗	✓
CVE-2025-24063	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Windows Kernel	✗	✗	✓
CVE-2025-29971	Web Threat Defense (WTD.sys) Denial of Service Vulnerability	Web Threat Defense (WTD.sys)	✗	✗	✓
CVE-2025-30382	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	✗	✗	✓
CVE-2025-30385	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	✗	✗	✓
CVE-2025-30388	Windows Graphics Component Remote Code Execution Vulnerability	Windows Win32K - GRFX	✗	✗	✓

Vulnerability Details

#1

Microsoft's May 2025 Patch Tuesday delivers fixes for 83 vulnerabilities, including 11 rated critical and 66 of important severity. Notably, five zero-day flaws currently being actively exploited in the wild have been addressed in this update.

#2

This month's security release tackles a broad spectrum of threats, comprising 29 Remote Code Execution (RCE) vulnerabilities, 20 Elevation of Privilege (EoP) flaws, 16 Information Disclosure issues, 7 Denial of Service (DoS) vulnerabilities, 2 Security Feature Bypass bugs, and 4 Spoofing vulnerabilities.

#3

Among the most critical fixes is CVE-2025-30400, a vulnerability actively weaponized in the wild. It involves a use-after-free flaw in Windows Desktop Window Manager (DWM), which allows an attacker with local access to escalate privileges to SYSTEM, potentially seizing control of vital system resources.

#4

Two other serious issues, CVE-2025-32701 and CVE-2025-32706, affect the Common Log File System (CLFS) driver, which underpins transactional logging for numerous Windows services. CVE-2025-32701 is another use-after-free vulnerability, enabling local privilege escalation, while CVE-2025-32706 stems from improper input validation, also allowing authenticated attackers to obtain SYSTEM privileges.

#5

CVE-2025-32709 impacts the Windows Ancillary Function Driver (AFD), a kernel-mode driver integral to the Windows Sockets (Winsock) API, managing the interface between applications and the network stack. This use-after-free vulnerability can similarly be exploited by an authenticated attacker to gain SYSTEM-level privileges.

#6

Another high-risk flaw, CVE-2025-30397, targets the Windows Scripting Engine. It's a memory corruption issue that permits RCE if a user is enticed into opening a malicious link, posing a serious threat for browser-based attacks and email phishing campaigns.

#7

Finally, CVE-2025-32702 presents a significant concern for developer environments. This RCE vulnerability affects Visual Studio and could be exploited to run arbitrary code with the privileges of the targeted user. Given that development systems often have elevated permissions and access to sensitive assets like cloud credentials and CI/CD pipelines, this flaw represents a potential risk to software supply chain security.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-30400	Windows: 10 21H2 - 11 24H2 Windows Server: 2012 Gold - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-416
CVE-2025-32701	Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-416
CVE-2025-32706	Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-20
CVE-2025-32709	Windows: 10 21H2 - 11 24H2 Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-416
CVE-2025-30397	Windows: 10 - 11 Windows Server: 2008 - 2025 Microsoft Internet Explorer: 11	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_internet_explorer:-:*:*:*:*:*:*:*	CWE-843
CVE-2025-32702	Visual Studio: 15.9 - 17.13.6	cpe:2.3:a:microsoft:visual_studio:-:*:*:*:*:*:*:*	CWE-77
CVE-2025-30386	Microsoft Office: 2016 - 2019 Microsoft Office LTSC: 2021 - 2024 for Mac Microsoft Office for Android: All versions Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	cpe:2.3:a:microsoft:microsoft_office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_office_for_android:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_365_apps_for_enterprise:-:*:*:*:*:*:*:*	CWE-416
CVE-2025-26685	Microsoft Defender for Identity: All versions	cpe:2.3:a:microsoft:microsoft_defender_for_identity:*:*:*:*:*:*:*:*	CWE-287
CVE-2025-29967	Windows: 10 21H2 - 11 24H2 Windows Server: 2008 R2 SP1 - 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-2025-24063	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-122
CVE-2025-29971	Windows: 10 1607 - 11 24H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-125
CVE-2025-30382	Microsoft SharePoint Server: 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016	cpe:2.3:a:microsoft:microsoft_sharepoint_server:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_sharepoint_server_subscription_edition:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_sharepoint_enterprise_server:-:*:*:*:*:*:*:*	CWE-502
CVE-2025-30385	Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-416
CVE-2025-30388	Microsoft Office for Mac Microsoft Office for Android Microsoft Office for Universal Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:a:microsoft:microsoft_office_for_mac:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_office_for_android:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-122

Recommendations

Review and harden system configurations, especially on internet-facing servers, endpoints, and development tools. Disable or restrict unnecessary services and apply additional security controls like exploit protection and application whitelisting.

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 other security measures.

Maintain a robust vulnerability management program to continuously track, prioritize, and remediate high-severity and actively exploited vulnerabilities in alignment with threat intelligence updates.

Enforce strict privilege management policies by adhering to the principle of least privilege. Limit administrative rights and ensure users only have the access required for their specific roles, reducing potential impact from privilege escalation vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0040** Impact	**T1068** Exploitation for Privilege Escalation	**T1203** Exploitation for Client Execution
T1498 Network Denial of Service	**T1190** Exploit Public-Facing Application	**T1210** Exploitation of Remote Services	**T1566.002** Spearphishing Link
T1195.002 Compromise Software Supply Chain	**T1078** Valid Accounts	**T1204.001** Malicious Link	**T1059** Command and Scripting Interpreter
T1040 Network Sniffing	**T1566** Phishing	**T1195** Supply Chain Compromise	**T1204** User Execution

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30400

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32701

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32706

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32709

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30397

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32702

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30386

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-26685

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-29967

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-24063

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-29971

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30382

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30385

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30388

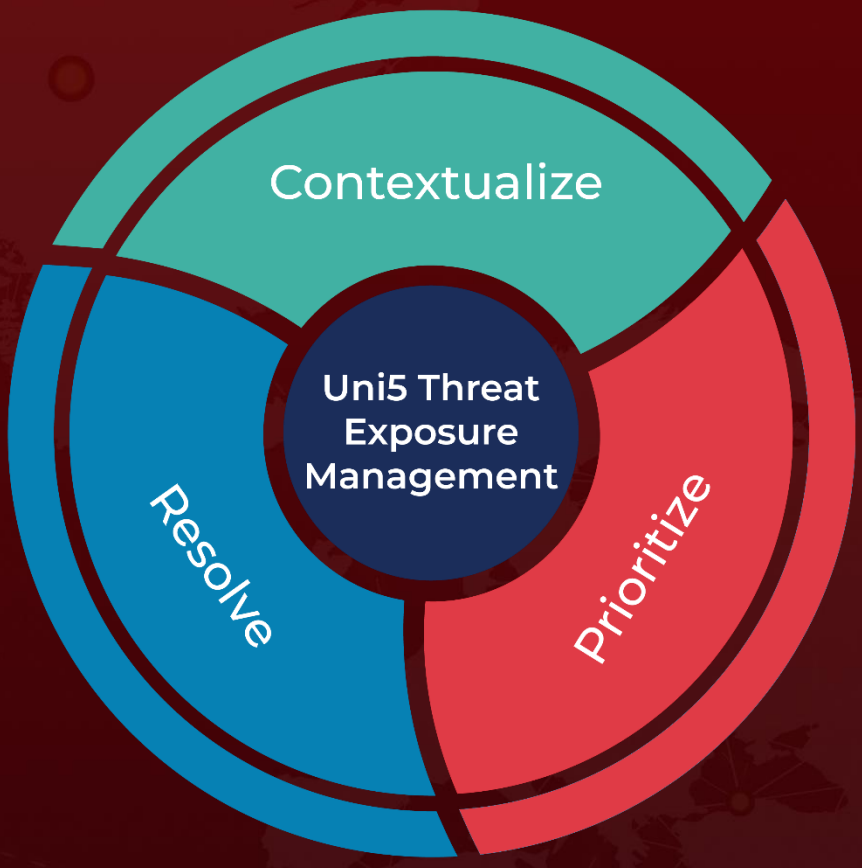
References

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

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

May 15, 2025 • 9:00 PM

More at www.hivepro.com