Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

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

Date of Publication	Admiralty Code	TA Number
June 12, 2025	A1	TA2025184

Summary

First Seen: June 10, 2025
Affected Platforms: Microsoft Windows, Microsoft Office, Windows Kernel, Windows Remote Desktop Services, Windows Storage Management Provider, Microsoft Office SharePoint, and more.
Impact: Denial of Service (DoS), Elevation of Privilege (EoP), Remote Code Execution (RCE), Information Disclosure, Security Feature Bypass and Spoofing.
Threat Actor: Stealth Falcon (aka FruityArmor, Project Raven, G0038)

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-33053	Web Distributed Authoring and Versioning (WebDAV) External Control of File Name or Path Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-33073	Windows SMB Client Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-32713	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-32714	Windows Installer Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-32717	Microsoft Word Remote Code Execution Vulnerability	Microsoft Word	✗	✗	✓
CVE-2025-33070	Windows Netlogon Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-33071	Windows KDC Proxy Service (KPSSVC) Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-47162	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	✗	✗	✓
CVE-2025-47164	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	✗	✗	✓
CVE-2025-47167	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	✗	✗	✓
CVE-2025-47962	Windows SDK Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-29828	Windows Schannel Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-32710	Windows Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-47172	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	✗	✗	✓
CVE-2025-47953	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	✗	✗	✓
CVE-2025-47966	Power Automate Elevation of Privilege Vulnerability	Power Automate	✗	✗	✓
CVE-2025-32711	EchoLeak (M365 Copilot Information Disclosure Vulnerability)	Microsoft 365 Copilot	✗	✗	✓

Vulnerability Details

#1

Microsoft's June 2025 Patch Tuesday includes security updates for 68 vulnerabilities, classified as 12 Critical and 56 Important. These encompass 26 Remote Code Execution, 14 Elevation of Privilege, 18 Information Disclosure, 6 Denial of Service, 2 Security Feature Bypass, and 2 Spoofing vulnerabilities. The updates apply to a broad range of Microsoft products, including Windows, Office, Visual Studio, Windows Remote Desktop Services, Microsoft 365 Copilot, Windows Storage Management Provider, and other components.

#2

Notably, Microsoft also patched three non-Microsoft vulnerabilities, one assigned to Windows by CERT, and two assigned by Google Chrome affecting the Chromium-based Microsoft Edge browser. This brings the total number of CVEs addressed to 71. This advisory addresses 17 CVEs with potential exploitation risks.

#3

The update includes one actively exploited zero-day vulnerability: CVE-2025-33053, a Remote Code Execution flaw in WebDAV. It allows attackers to execute arbitrary code by manipulating file names or paths. Notably, it's been attributed to Stealth Falcon, an APT group targeting government and defense entities across the Middle East and Africa, including Turkey, Qatar, Egypt, and Yemen, using phishing emails disguised as military documents.

#4

Another critical vulnerability, CVE-2025-33073, was publicly disclosed prior to patching. Although not yet known to be actively exploited, it is considered high-risk. Successful exploitation could allow an attacker to gain SYSTEM-level privileges. One attack scenario involves coercing a victim system into connecting to a malicious SMB server, where the attacker could leverage the connection to escalate privileges and execute arbitrary code.

#5

CVE-2025-32711 (EchoLeak), a Critical AI command injection vulnerability in Microsoft 365 Copilot. This zero-click flaw allowed unauthorized attackers to exfiltrate context-sensitive data from Copilot without any user interaction. Microsoft patched it server-side, so no customer action was needed

#6

Several Microsoft Office RCE vulnerabilities were also addressed, including CVE-2025-47162, CVE-2025-47164, CVE-2025-47167, and CVE-2025-47953. Beyond Office, other significant vulnerabilities include CVE-2025-47962 is an elevation-of-privilege vulnerability in the Windows SDK that allows a locally authorized attacker to gain higher privileges by exploiting improper access controls, and CVE-2025-29828, which affects Windows' Schannel. These vulnerabilities underscore the importance of applying the June 2025 patches to protect against potential exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-33053	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-73
CVE-2025-33073	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-284
CVE-2025-32713	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-32714	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-284
CVE-2025-32717	Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-33070	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-908
CVE-2025-33071	Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-47162	Microsoft Office 2016 & 2019 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office_ltsc:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-47164	Microsoft Office 2016 & 2019 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office_ltsc:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-47167	Microsoft Office 2016 & 2019 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office_ltsc:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:*	CWE-843
CVE-2025-47962	Windows SDK	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-284
CVE-2025-29828	Windows: 11 22H2 - 24H2 Windows Server: 2022 & 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-401
CVE-2025-32710	Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416 CWE-362
CVE-2025-47172	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-47953	Microsoft Office 2016 & 2019 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office_ltsc:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:*	CWE-641
CVE-2025-47966	Power Automate for Desktop	cpe:2.3:a:microsoft:power_automate_for_desktop:*:*:*:*:*:*:*:*	CWE-200
CVE-2025-32711	Microsoft 365 Copilot	cpe:2.3:a:microsoft:365_copilot:*:*:*:*:*:*:*:*	CWE-77

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-2025-33053, and publicly disclosed CVE-2025-33073. 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

TA0042 Resource Development	TA0040 Impact	TA0005 Defense Evasion	TA0002 Execution
TA0001 Initial Access	TA0004 Privilege Escalation	TA0008 Lateral Movement	TA0003 Persistence
T1204 User Execution	T1566 Phishing	T1059 Command and Scripting Interpreter	T1189 Drive-by Compromise
T1204.002 Malicious File	T1021.002 SMB/Windows Admin Shares	T1021 Remote Services	T1588.005 Exploits
T1556 Modify Authentication Process	T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	T1068 Exploitation for Privilege Escalation
T1498 Network Denial of Service	T1210 Exploitation of Remote Services	T1588 Obtain Capabilities	T1588.006 Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	ba5beb189d6e1811605b0a4986b232108d6193dcf09e5b2a603ea4448e6f263c, e0a44274d5eb01a0379894bb59b166c1482a23fede1f0ee05e8bf4f7e4e2fcc6, da3bb6e38b3f4d83e69d31783f00c10ce062abd008e81e983a9bd4317a9482aa, ddce79afe9f67b78e83f6e530c3e03265533eb3f4530e7c89fdc357f7093a80b, 1d95a44f341435da50878eea1ec0a1aab6ae0ee91644c497378266290a6ef1d8, 700b422556f070325b327325e31ddf597f98cc319f29ef8638c7b0508c632cee,

TYPE	VALUE
SHA256	aa612f53e03539cdc8f8a94deee7bf31f0ac10734bb9301f4506b9113c691c97, 66a893728a0ac1a7fae39ee134ad4182d674e719219fbf5d9b7cd4fd4f07f535, cd6335101e0187c33a78a316885a2cbf4cbbd2a72daf64a086edb4a2615749fb, 257c63a9e21b829bb4b9f8b0e352379444b0e573176530107a3e6c279d1919da, 5671b3a89c0e88a9bfb0bd5bc434fa5245578becfdeb284f4796f65eecbd6f15, 3259ecfb96d3d7e2d1a782b01073e02b3488a3922fd2fd35c20eeb5f44b292ec, 8065c85e387654cb79a12405ff0f99fd4ddd5a5d3b9876986b82822bd10c716f, 0598e1af6466b0813030d44fa64616eea7f83957d70f2f48376202c3179bd6b1, f270202cd88b045630f6d2dec6d5823aa08aa66949b9ccd20f6e924c7992fea7, 092c344330bd5cba71377dead11946f7277f2dd4af57f5b636b70b343bc7ebe0, dc7cb53c5dc2e756822328a7144c29318cb871890727eff9c8da64a01e8e782d, db7364296cc8f78981797ffb2af7063bba97e2f6631c29215d59f4979f8b4fce, 4e045c83cf429210e71e324adccad8818540b9805a44c8d79a8c16c3d5f6fbb6, 62797e28a334e392cb56fcc26dd07f04ac031110f0e9ed8489ec0825beea75eb, dec6dda0559e381c23f1dfbe92fa4705c8455430f8278c78c170a7533b703296, 32f2773ceb6503f8a1c3e456d34ceda5c188974a115e5225a1315e7ec3f8eb5e, 50a2b6c1b0a0d308e8016aece9629c1bf6ca4ecc6f4cef34c904e9c3e82355fb, 9ed8f51548a004ac61b7176df12a0064dc3096088cbf3c644a9abdb5c92936f7, 9a82e21c2463d6c23a48409a862e668ed9c205468d216d2280f7debe1ab1ddd8, 46c95af6fea41b55fa0ab919ec81d38a584e32a519f85812fe79a5379457f111, c5b00e8312e801dc35652c631a14270ed4eec8f6d90d08cdde3c6e7fd1ec24b6, 3b83250383c2a892e0ca86e54fcc6aca9960fc4b425ab9853611ff3e5aa2f9c6, 8291b886cce1f0474db5b3dc269adf31d1659b7d949f62ea23608409d14b9ceb

TYPE	VALUE
Domains	roundedbullets[.]com, summerartcamp[.]net, downloadessays[.]net, joinushealth[.]com, healthherofit[.]com, worryfreetransport[.]com, radiotimesignal[.]com, fastfilebackup[.]com, cyclingonlineshop[.]com, luxuryfitnesslabs[.]com, purvoyage[.]com

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32713

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32714

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32717

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33070

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33071

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47162

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47164

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47167

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47962

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29828

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32710

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47172

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47953

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47966

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32711

References

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

https://research.checkpoint.com/2025/stealth-falcon-zero-day/

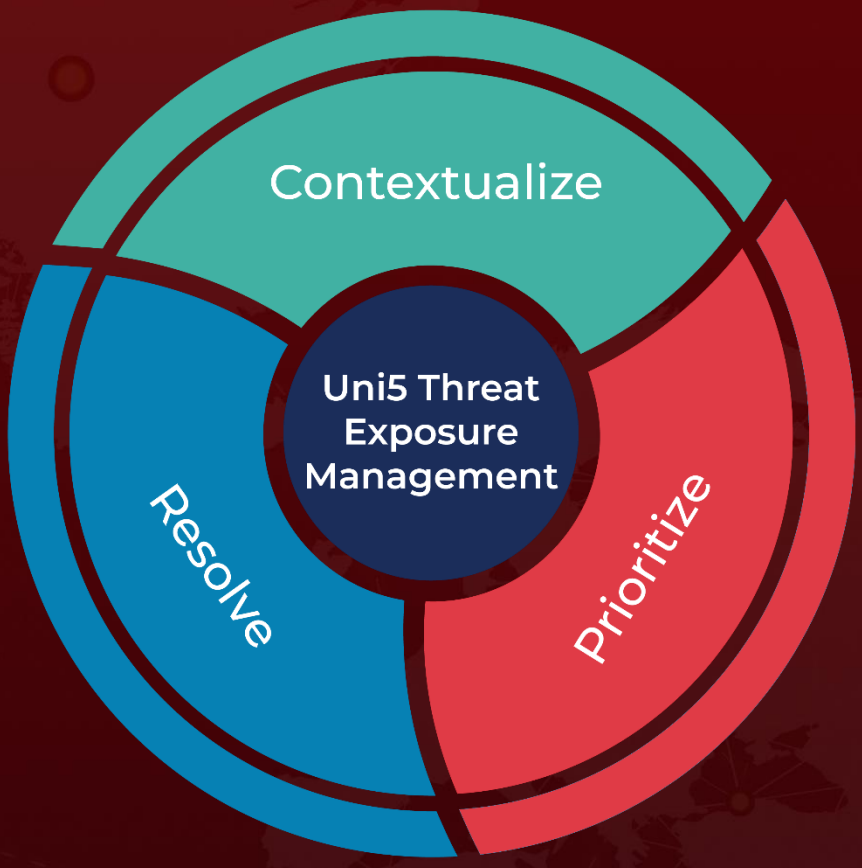
https://hivepro.com/threat-advisory/deadglyph-malware-emerges-as-a-game-changer-for-stealth-falcon/

https://windowsforum.com/threads/echoleak-zero-click-vulnerability-in-microsoft-365-copilot-threatens-enterprise-data-security.370055/?utm_source=rss&utm_medium=rss

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

June 12, 2025 • 7:30 AM

More at www.hivepro.com