Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft’s November Patch Tuesday Addresses Active Zero-Day Exploits

Date of Publication	Admiralty Code	TA Number
November 13, 2024	A1	TA2024429

Summary

First Seen: November 12, 2024
Affected Platforms: Microsoft Windows, Windows Task Scheduler, Microsoft Office, Microsoft Azure, Microsoft Word, Microsoft Visual Studio, Microsoft Active Directory, and more.
Impact: Denial of Service (DoS), Elevation of Privilege (EoP), Remote Code Execution (RCE), Information Disclosure, Spoofing, and Security Feature Bypass.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-49039	Windows Task Scheduler Elevation of Privilege Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-43451	NTLM Hash Disclosure Spoofing Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-43623	Windows NT OS Kernel Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-43629	Windows DWM Core Library Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-43630	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-43636	Win32k Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-43642	Windows SMB Denial of Service Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49019	Active Directory Certificate Services Elevation of Privilege Vulnerability	Microsoft Active Directory	✗	✗	✓
CVE-2024-49033	Microsoft Word Security Feature Bypass Vulnerability	Microsoft Word	✗	✗	✓
CVE-2024-49040	Microsoft Exchange Server Spoofing Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2024-43498	.NET and Visual Studio Remote Code Execution Vulnerability	Microsoft .NET and Visual Studio	✗	✗	✓
CVE-2024-43625	Microsoft Windows VMSwitch Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-43639	Windows Kerberos Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49056	Airlift.microsoft.com Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✗

Vulnerability Details

#1

Microsoft's November 2024 Patch Tuesday includes security updates for 89 vulnerabilities, classified into 4 critical, 84 important, and 1 moderate-severity vulnerabilities. These encompass 51 Remote Code Execution, 28 Elevation of Privilege, 4 Denial of Service, 3 Spoofing, 2 Security Feature Bypass, and 1 Information Disclosure vulnerability.

#2

The updates apply to a broad range of Microsoft products, including Windows, Office, .NET, Visual Studio, Azure, SQL Server, Windows Task Scheduler, Windows Hyper-V, Microsoft Exchange Server, and other components. Notably, Microsoft also patched three non-Microsoft vulnerabilities, including one for Microsoft Defender for Endpoint via OpenSSL, and two affecting the Chromium-based Microsoft Edge browser, bringing the total CVE count to 92. This advisory addresses 14 CVEs with potential exploitation risks.

#3

The update mitigates two actively exploited zero-day vulnerabilities and two others that were publicly disclosed. The first active exploit, CVE-2024-49039, affects Windows Task Scheduler, allowing attackers to escalate privileges on compromised systems. The second, CVE-2024-43451, is a spoofing vulnerability in NTLM hash disclosure, enabling attackers to access NTLM hashes with minimal user interaction. Linked to phishing attacks targeting Ukrainian entities, this flaw highlights its potential impact on system security through unauthorized impersonation.

#4

Additionally, Microsoft patched two other publicly disclosed vulnerabilities, CVE-2024-49040, a spoofing flaw in Microsoft Exchange Server that lets attackers impersonate email sender addresses, and CVE-2024-49019, an elevation of privilege vulnerability in Active Directory Certificate Services. These underscore the importance of timely updates to protect systems from potential exploitation.

#5

Among the resolved vulnerabilities, SQL Server stands out, with at least 30 CVEs identified, primarily involving remote code execution risks in SQL Server Native Client. Attackers could exploit these by convincing users to connect to a malicious SQL Server database, potentially enabling arbitrary code execution on the user's machine.

#6

November's Patch Tuesday emphasizes the need for prompt patching to reduce risks, particularly for actively exploited vulnerabilities, thereby ensuring system integrity and protection.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-49039	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-287
CVE-2024-43451	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-73
CVE-2024-43623	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-190
CVE-2024-43629	Windows: 10 - 11 24H2 Windows Server: 2019 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-822
CVE-2024-43630	Windows: 10 - 11 24H2 Windows Server: 2022 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-121
CVE-2024-43636	Windows: 10 - 11 24H2 Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-822
CVE-2024-43642	Windows: 11 - 11 24H2 Windows Server: 2022 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-49019	Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-1390

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-49033	Microsoft Office 2019 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise Microsoft Word 2016	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:word:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-49040	Microsoft Exchange Server 2016 & 2019	cpe:2.3:a:microsoft:exchange_server:2016:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:*:*:*:*:*:*:*	CWE-451
CVE-2024-43498	.NET 9.0 and Microsoft Visual Studio 2022	cpe:2.3:a:microsoft:.net:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio:*:*:*:*:*:*:*:*	CWE-843
CVE-2024-43625	Windows: 11 - 11 24H2 Windows Server: 2022 & 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-43639	Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-197
CVE-2024-49056	airlift.microsoft.com	cpe:2.3:a:microsoft:airlift.microsoft.com:*:*:*:*:*:*:*:*	CWE-302

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 actively exploited vulnerabilities CVE-2024-43451 and CVE-2024-49039, along with the publicly disclosed CVE-2024-49019, and CVE-2024-49040. These vulnerabilities have the potential for severe exploitation 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	T1588 Obtain Capabilities	T1588.005 Exploits
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	T1204.001 Malicious Link

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49039

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43623

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43629

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43630

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43636

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43642

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49019

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49033

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49040

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43498

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43625

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43639

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49056

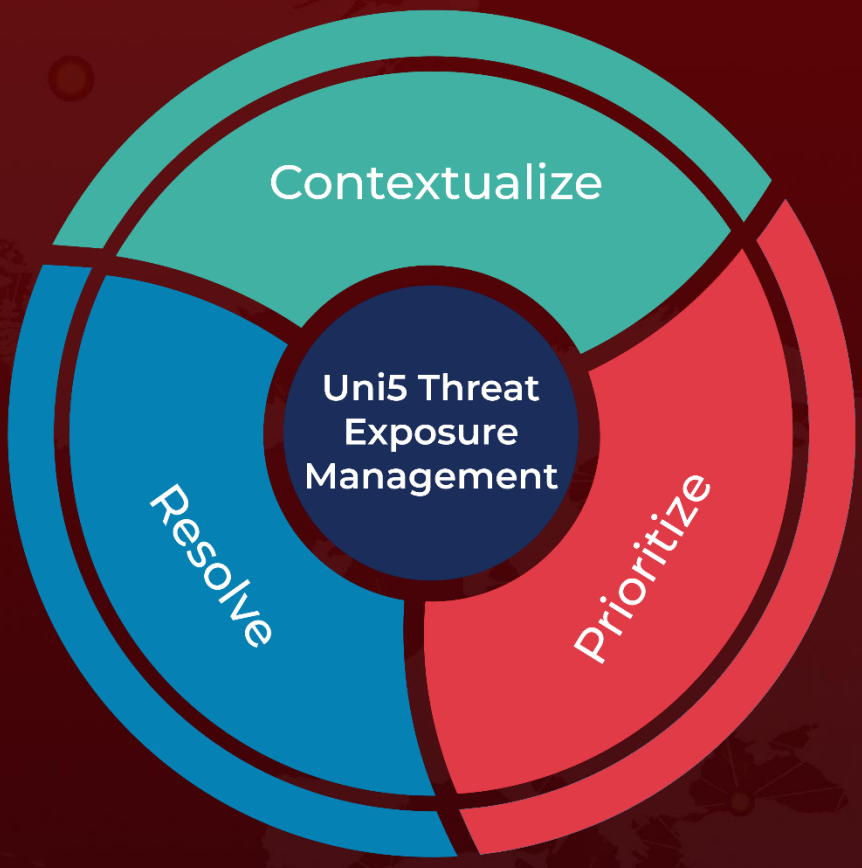
References

https://msrc.microsoft.com/update-guide/releaseNote/2024-nov

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

November 13, 2024 . 11:30 PM

More at www.hivepro.com