Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's December 2024 Patch Tuesday Addresses 72 Vulnerabilities

Date of Publication	Admiralty Code	TA Number
December 12, 2024	A1	TA2024460

Summary

First Seen: December 10, 2024
Affected Platforms: Microsoft Windows, Microsoft SharePoint, Windows Task Scheduler, Microsoft Office, Microsoft Excel, Microsoft Word, Microsoft Defender for Endpoint and more.
Impact: Denial of Service (DoS), Elevation of Privilege (EoP), Remote Code Execution (RCE), Information Disclosure, and Spoofing.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-49138	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-49070	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✗	✓
CVE-2024-49088	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49090	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49093	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-49114	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49122	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49117	Windows Hyper-V Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49126	Windows Local Security Authority Subsystem Service (LSASS) Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49118	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49112	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49127	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-49124	Lightweight Directory Access Protocol (LDAP) Client Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓

Vulnerability Details

#1

Microsoft's December 2024 Patch Tuesday includes security updates for 72 vulnerabilities, classified into 17 critical, 54 important, and 1 moderate-severity vulnerability. These encompass 31 Remote Code Execution, 27 Elevation of Privilege, 7 Information Disclosure, 5 Denial of Service, and 2 Spoofing vulnerabilities.

#2

The updates apply to a broad range of Microsoft products, including Windows, Office, Windows Remote Desktop Services, Windows Task Scheduler, Windows Hyper-V, Microsoft SharePoint, and other components. Notably, Microsoft also patched one non-Microsoft vulnerability affecting the Chromium-based Microsoft Edge browser, bringing the total CVE count to 73. This advisory addresses 13 CVEs with potential exploitation risks.

#3

This month's update includes a zero-day vulnerability, CVE-2024-49138, classified as an Elevation of Privilege vulnerability in the Windows Common Log File System (CLFS) Driver. This zero-day vulnerability is particularly alarming because it is actively being exploited in the wild. Attackers can leverage this flaw to gain SYSTEM privileges on affected devices, which could allow them to execute arbitrary code or take control of the system entirely.

#4

Among the critical vulnerabilities, Remote Code Execution (RCE) remains the most concerning. Notable CVEs include CVE-2024-49112 and CVE-2024-49127, both affecting LDAP. These flaws enable unauthenticated attackers to execute arbitrary code on servers by sending crafted LDAP requests.

#5

Furthermore, multiple Windows Remote Desktop Services (RDS) vulnerabilities involve race conditions that can lead to remote code execution by exploiting the Remote Desktop Gateway role. Microsoft also addressed CVE-2024-49070, a remote code execution vulnerability in SharePoint, and CVE-2024-49093, an elevation of privilege flaw in the Windows Resilient File System (ReFS).

#6

Additionally, CVE-2024-49117, which affects Windows Hyper-V, poses a significant risk by enabling guest VM users to execute code on the host system, endangering virtualized environments. Another noteworthy flaw is CVE-2024-49126, which allows attackers to achieve remote code execution via a race condition affecting the Local Security Authority Subsystem Service (LSASS). December's Patch Tuesday emphasizes the need for prompt patching to reduce risks, particularly for actively exploited and critical vulnerabilities, thereby ensuring system integrity and protection.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-49138	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2024-49070	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	cpe:2.3:o:microsoft:sharepointserver:*:*:*:*:*:*:*:*	CWE-502
CVE-2024-49088	Windows: 10 – 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-126
CVE-2024-49090	Windows: 10 – 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-822
CVE-2024-49093	Windows: 11 24H2 Windows Server: 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-681
CVE-2024-49114	Windows: 10 – 11 24H2 Windows Server: 2019 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-820
CVE-2024-49122	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-2024-49117	Windows: 11 22H2- 11 24H2 Windows Server: 2022 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-393
CVE-2024-49126	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416 CWE-591
CVE-2024-49118	Windows: 10 - 11 24H2 Windows Server: 2008 – 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-49112	Windows: 10 - 11 24H2 Windows Server: 2008 – 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-190
CVE-2024-49127	Windows: 10 - 11 24H2 Windows Server: 2008 – 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-49124	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-362

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-2024-49138 and the critical vulnerabilities CVE-2024-49112 and CVE-2024-49117. 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	**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	**T1210** Exploitation of Remote Services	**T1133** External Remote Services	

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49070

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49088

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49090

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49093

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49114

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49122

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49117

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49126

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49118

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49127

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49124

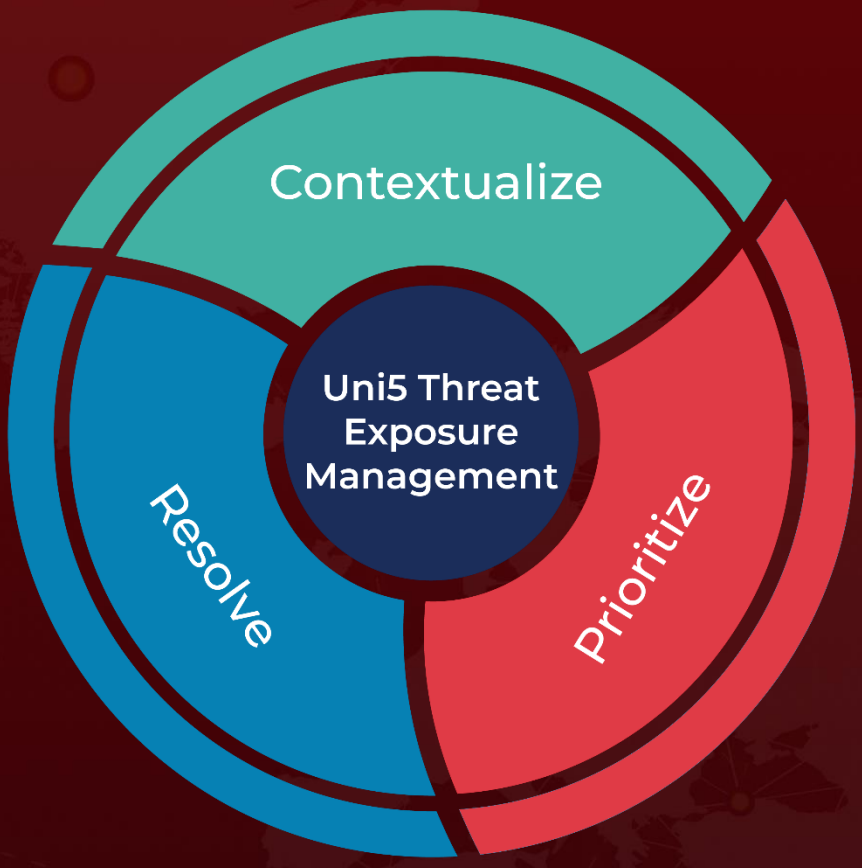
References

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

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

December 12, 2024 . 4:30 AM

More at www.hivepro.com