Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's August Patch Tuesday Addresses Active Zero-Day Exploits

Date of Publication	Admiralty Code	TA Number
August 16, 2024	A1	TA2024315

Summary

First Seen: August 13, 2024
Affected Platforms: Microsoft Windows, Windows Common Log File System Driver, Windows Kerberos, Microsoft Office, Microsoft Azure, Microsoft Outlook
Impact: Denial of Service (DoS), Elevation of Privilege (EoP), Remote Code Execution (RCE), Information Disclosure, Spoofing, Security Feature Bypass, and Tampering

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38106	Microsoft Windows Kernel Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-38107	Microsoft Windows Power Dependency Coordinator Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-38178	Microsoft Windows Scripting Engine Memory Corruption Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-38189	Microsoft Project Remote Code Execution Vulnerability	Microsoft Project	✓	✓	✓
CVE-2024-38193	Microsoft Windows Ancillary Function Driver for WinSock Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38213	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-21302	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	Windows Secure Kernel	✓	✗	✓
CVE-2024-38202	Windows Update Stack Elevation of Privilege Vulnerability	Microsoft Windows	✓	✗	✗
CVE-2024-38199	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability	Microsoft Windows	✓	✗	✓
CVE-2024-38200	Microsoft Office Spoofing Vulnerability	Microsoft Office	✓	✗	✓
CVE-2024-38063	Windows TCP/IP Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38125	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Microsoft Windows Kernel	✗	✗	✓
CVE-2024-38133	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38141	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38144	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Microsoft Windows Kernel	✗	✗	✓
CVE-2024-38147	Microsoft DWM Core Library Elevation of Privilege Vulnerability	Microsoft DWM Core Library	✗	✗	✓
CVE-2024-38148	Windows Secure Channel Denial of Service Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38150	Windows DWM Core Library Elevation of Privilege Vulnerability	Microsoft Windows DWM	✗	✗	✓
CVE-2024-38163	Windows Update Stack Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38196	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38198	Windows Print Spooler Elevation of Privilege Vulnerability	Microsoft Windows Print Spooler	✗	✗	✓

Vulnerability Details

#1 Microsoft's August 2024 Patch Tuesday includes security updates for a total of 89 vulnerabilities, comprising 7 critical, 81 important, and 1 moderate severity vulnerability. The breakdown of these vulnerabilities includes 36 Elevation of Privilege, 29 Remote Code Execution, 8 Information Disclosure, 7 Spoofing, 6 Denial of Service, 2 Security Feature Bypass, and 1 Tampering vulnerability.

#2

The updates cover a wide range of Microsoft products such as Windows, Office, .NET, Visual Studio, Azure, Copilot, Microsoft Dynamics, Teams, Secure Boot, and other components. Notably, Microsoft also patched twelve non-Microsoft vulnerabilities, including three assigned to Windows by Red Hat and nine affecting the Chromium-based Microsoft Edge browser, bringing the total number of CVEs to 101. This advisory pertains to 21 CVEs that could potentially be exploited.

#3

The update addresses six vulnerabilities that are actively being exploited and three that have been publicly disclosed as zero-days. Microsoft is still working on an update for a tenth publicly disclosed zero-day. This extensive patch cycle aims to address critical issues and enhance overall system security.

#4

The actively exploited zero-days addressed in this update include several high-impact vulnerabilities. For example, CVE-2024-38178 involves a scripting engine memory corruption flaw that requires an authenticated user to click a link in Edge's Internet Explorer mode. Similarly, CVE-2024-38193 and CVE-2024-38106 are elevation of privilege vulnerabilities allowing attackers to gain SYSTEM privileges, while CVE-2024-38189 pertains to remote code execution within Microsoft Project files, requiring specific security feature configurations to be disabled.

#5

Publicly disclosed vulnerabilities also received attention in this patch cycle. CVE-2024-38199 addresses a remote code execution flaw in the Windows Line Printer Daemon, while CVE-2024-21302 and CVE-2024-38202 are linked to elevation of privilege vulnerabilities exposed in recent Windows update downgrade attack demonstrations. CVE-2024-38200, a Microsoft Office spoofing vulnerability, exposes NTLM hashes and underscores the importance of securing Office files against phishing and other attacks.

#6

Patches for CVE-2024-38202, CVE-2024-38206, CVE-2024-38166, and CVE-2024-38109 are not yet available. Overall, this Patch Tuesday highlights Microsoft's ongoing efforts to address critical security concerns and mitigate risks associated with both actively exploited and publicly disclosed vulnerabilities. These fixes are crucial for maintaining system integrity and protecting against potential exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38106	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-591
CVE-2024-38107	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-38178	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-843
CVE-2024-38189	Microsoft Office LTSC 2021, Microsoft Project, Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:project:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-38193	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-38213	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-693
CVE-2024-21302	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-284

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38202	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-284
CVE-2024-38199	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-38200	Microsoft 365 Apps for Enterprise, Microsoft Office	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:*	CWE-200
CVE-2024-38063	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-191
CVE-2024-38125	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-197
CVE-2024-38133	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-138
CVE-2024-38141	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-38144	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-190

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38147	Windows: 10 - 11 23H2 Windows Server: 2022 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-38148	Windows: 10 - 11 23H2 Windows Server: 2022 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-125
CVE-2024-38150	Windows: 10 - 11 23H2 Windows Server: 2022 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-38163	Windows: 10 - 11 23H2 Windows Server: 2022	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-284
CVE-2024-38196	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-38198	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-345

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 actively exploited zero-day vulnerabilities, especially CVE-2024-38106, CVE-2024-38107, CVE-2024-38178, CVE-2024-38189, CVE-2024-38193, and CVE-2024-38213, which have also been added to the CISA KEV catalog. These vulnerabilities have the potential for severe exploitation and should be addressed urgently.

Keep an eye out for further updates from Microsoft, particularly for pending vulnerabilities like CVE-2024-38202, CVE-2024-38206, CVE-2024-38166, and CVE-2024-38109. Apply these patches promptly to maintain full protection.

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
TA0005 Defense Evasion	**T1498** Network Denial of Service	**T1588** Obtain Capabilities	**T1588.005** Exploits
T1059 Command and Scripting Interpreter	**T1588.006** Vulnerabilities	**T1068** Exploitation for Privilege Escalation	**T1203** Exploitation for Client Execution
T1495 Firmware Corruption	**T1133** External Remote Services		

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38125

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38133

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38141

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38144

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38147

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38148

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38150

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38163

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38196

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38198

References

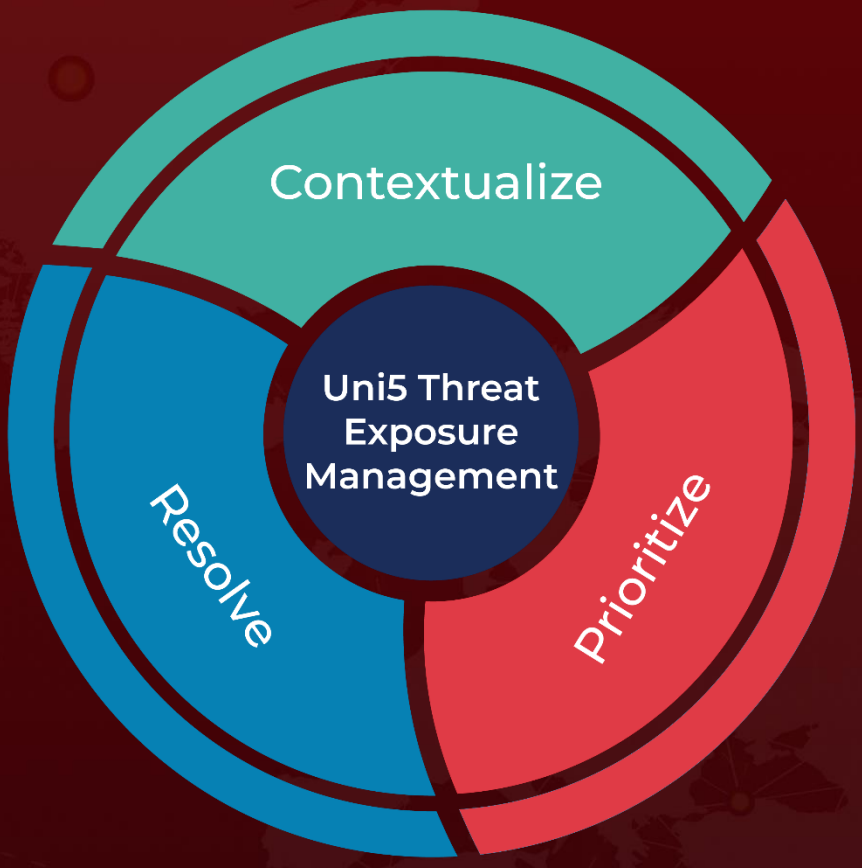
https://msrc.microsoft.com/update-guide/releaseNote/2024-aug

https://hivepro.com/threat-advisory/windows-update-zero-day-flaws-allow-downgrade-attacks-on-patched-systems/

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

August 16, 2024 • 6:30 AM

More at www.hivepro.com