

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Microsoft's November 2023 Patch Tuesday Addresses Five Zero-day Vulnerabilities

Date of Publication

November 15, 2023

Admiralty Code

A1

TA Number

TA2023460






















Summary

First Seen: November 14, 2023

Affected Platforms: Microsoft ASP.NET, Microsoft Office, Microsoft Windows, Microsoft Exchange Server, Microsoft Azure

Impact: Privilege Escalation, Remote Code Execution, Information Disclosure, Denial of Service, and Security Feature Bypass

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-36033	Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability	Microsoft Windows			
CVE-2023-36025	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows			
CVE-2023-36036	Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability	Microsoft Windows			
CVE-2023-36038	ASP.NET Core Denial of Service Vulnerability	Microsoft ASP.NET			
CVE-2023-36413	Microsoft Office Security Feature Bypass Vulnerability	Microsoft Office			
CVE-2023-36439	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server			
CVE-2023-36052	Microsoft Azure CLI REST Command Information Disclosure Vulnerability	Microsoft Azure			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-36400	Microsoft Windows HMAC Key Derivation Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2023-36397	Microsoft Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓

Vulnerability Details

#1

Microsoft's November 2023 Patch Tuesday includes security updates for 63 flaws, with five zero-day vulnerabilities actively exploited. Among these flaws, three are rated 'Critical,' while the remaining 60 are rated as 'Important.' The breakdown of vulnerabilities includes 16 Elevation of Privilege, 6 Security Feature Bypass, 15 Remote Code Execution, 6 Information Disclosure, 5 Denial of Service, 11 Spoofing vulnerabilities.

#2

In addition, one Mitre and fourteen Chromium-based Microsoft edge vulnerabilities were fixed. Microsoft also released non-security updates, including cumulative updates for Windows 11 and Windows 10. This advisory pertains to 9 CVEs that hold considerable potential for exploitation.

#3

CVE-2023-36413 exposes a flaw in Microsoft Office, allowing attackers to bypass Protected View, opening files in edit mode by convincing users to open malicious files. CVE-2023-36036 involves a Windows Cloud Files Mini Filter Driver vulnerability, enabling attackers to elevate privileges. CVE-2023-36038 highlights a Denial of Service risk in ASP.NET Core, specifically impacting .NET 8 RC 1 on IIS InProcess. Additionally, CVE-2023-36033 reveals a Windows DWM Core Library vulnerability that could lead to privilege escalation.

#4

Lastly, CVE-2023-36025 exposes a SmartScreen Security Feature Bypass, requiring users to click on crafted URLs, potentially compromising system security. These vulnerabilities underscore the need for prompt updates and user vigilance to mitigate potential exploitation. Microsoft has issued updates to address these issues and recommends applying them promptly to secure systems.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-36033	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-119
CVE-2023-36025	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-254
CVE-2023-36036	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-119
CVE-2023-36038	Visual Studio: 2022 version 17.2 - 2022 version 17.7 ASP.NET Core: 8.0 .NET: 8.0.0	cpe:2.3:a:microsoft:visual_studio:2022:version 17.7:*:*:*:*:*	CWE-20
CVE-2023-36413	Microsoft Office: 2016 - 2019 Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	cpe:2.3:a:microsoft:microsoft_office:2019:*:*:*:*:*	CWE-254
CVE-2023-36439	Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018	cpe:2.3:a:microsoft:microsoft_exchange_server:2019 CU12 Oct23SU:15.02.1118.039:*:*:*:*:*	CWE-502
CVE-2023-36397	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-20

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-36052	az webapp config appsettings set & delete: All versions; az staticwebapp appsettings set & delete: All versions; az logicapp config appsettings set & delete: All versions; az functionapp config appsettings set & delete: All versions	cpe:2.3:a:microsoft:az_webapp_config_appsettings_set:*:*:*:*:*:*	CWE-200
CVE-2023-36400	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-264

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.



Pay special attention to the five zero-day vulnerabilities actively exploited. Immediate patching is crucial to prevent potential exploitation and safeguard systems against malicious activities.



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

<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development	<u>TA0007</u> Discovery	<u>TA0002</u> Execution
<u>TA0003</u> Persistence	<u>TA0040</u> Impact	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits
<u>T1059</u> Command and Scripting Interpreter	<u>T1588.006</u> Vulnerabilities	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1203</u> Exploitation for Client Execution
<u>T1082</u> System Information Discovery	<u>T1498</u> Network Denial of Service		

Patch Details

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36033>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36036>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36038>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36413>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36439>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36052>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36400>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36397>

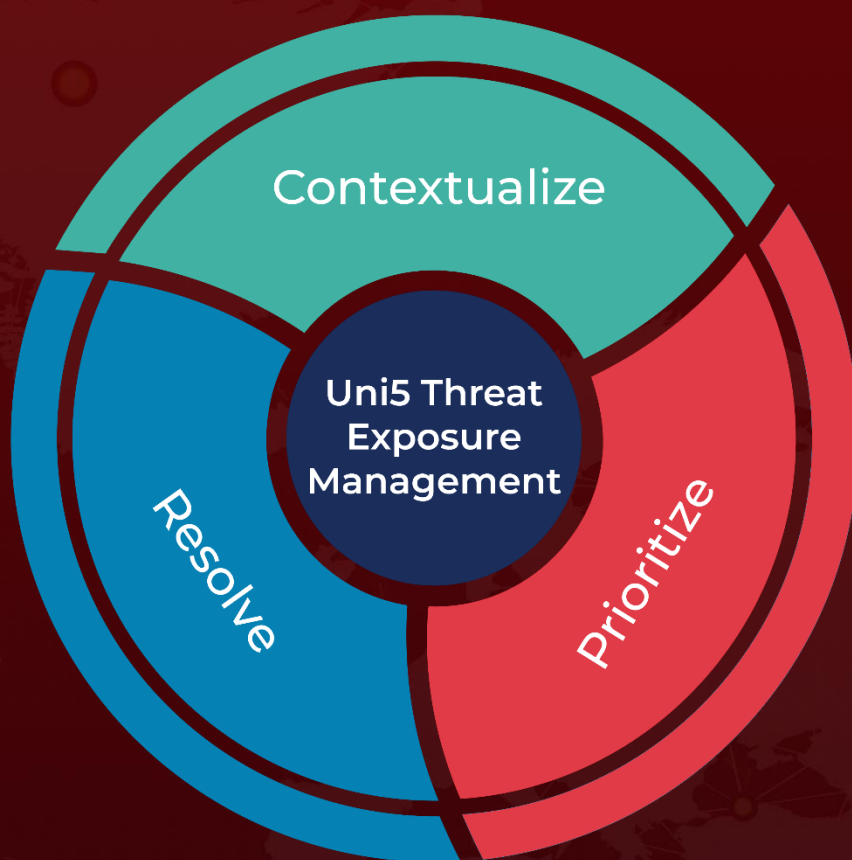
References

<https://msrc.microsoft.com/update-guide/releaseNote/2023-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 15, 2023 • 4:30 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com