

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Microsoft's December 2023 Patch Tuesday Addresses One Zero-day Vulnerability

Date of Publication

December 13, 2023

Admiralty Code

A1

TA Number

TA2023502



















Summary

First Seen: December 12, 2023

Affected Platforms: Microsoft Azure, Microsoft Office and Components, Windows Win32K, Windows Kernel, Microsoft Bluetooth Driver, Windows DHCP Server, Windows ODBC Driver, and more

Impact: Denial of Service (DoS), Elevation of Privilege (EoP), Information Disclosure, Remote Code Execution (RCE), and Spoofing

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-20588	AMD Speculative Execution information disclosure Vulnerability	Microsoft Windows			
CVE-2023-36019	Microsoft Azure Logic Apps/Power Platform Remote Code Execution Vulnerability	Microsoft Azure			
CVE-2023-35630	Microsoft Windows Internet Connection Sharing Remote Code Execution Vulnerability	Microsoft Windows			
CVE-2023-35641	Microsoft Windows Internet Connection Sharing Remote Code Execution Vulnerability	Microsoft Windows			
CVE-2023-35628	Microsoft Windows MSHTML Platform Remote Code Execution Vulnerability	Microsoft Windows			
CVE-2023-35636	Microsoft Office Outlook Information Disclosure Vulnerability	Microsoft Office Outlook			

Vulnerability Details

#1

Microsoft's December 2023 Patch Tuesday includes security updates for 42 flaws, with one zero-day vulnerability. Among these flaws, four are rated as 'Critical,' one is rated as 'Moderate,' and two are rated as 'Low'. The severity of five CVEs is unknown, while the remaining 30 are rated as 'Important.' The breakdown of vulnerabilities includes 11 Elevation of Privilege, 8 Remote Code Execution, 8 Information Disclosure, 5 Denial of Service, and 5 Spoofing vulnerabilities.

#2

Five Chromium-based Microsoft Edge vulnerabilities were also fixed. Notably, a zero-day vulnerability (CVE-2023-20588) affecting some AMD processors was patched, addressing a division-by-zero error that could potentially lead to the disclosure of speculative data. This advisory pertains to 6 CVEs that hold considerable potential for exploitation.

#3

Several Critical Severity Vulnerabilities were also addressed, such as a Microsoft Power Platform Connector Spoofing Vulnerability (CVE-2023-36019) and Internet Connection Sharing (ICS) Remote Code Execution Vulnerabilities (CVE-2023-35630, CVE-2023-35641). The Microsoft MSHTML Platform also had a Critical Remote Code Execution Vulnerability (CVE-2023-35628), which could be exploited via a specially crafted email.

#4

Various Elevation of Privilege Vulnerabilities were fixed across different components, including Windows Kernel, Ancillary Function Driver (AFD) for Winsock, Win32k, Sysmain Service, Windows Telephony Server, Local Security Authority Subsystem Service, and Windows Cloud Files Mini Filter Driver.

#5

Overall, Microsoft's Patch Tuesday for December 2023 is characterized by a lighter set of updates, including various critical and important fixes, with a focus on addressing potential security risks in a variety of products.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-20588	Windows Server: 2008 - 2022 23H2 Windows: 10 - 11 23H2	cpe:2.3:o:microsoft:windows_server:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*	CWE-369
CVE-2023-36019	Microsoft Power Platform: All versions Azure Logic Apps: All versions	cpe:2.3:a:microsoft:microsoft_power_platform:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_logic_apps:*:*:*:*:*	CWE-451
CVE-2023-35630	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*	CWE-20
CVE-2023-35641	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*	CWE-20
CVE-2023-35628	Windows: 10 - 11 23H2 Windows Server: 2008 R2 - 2022 23H2 Microsoft Internet Explorer: 11 - 11.1790.17763.0	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:* cpe:2.3:o:microsoft:microsoft_internet_explorer:*:*:*:*:*	CWE-20
CVE-2023-35636	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:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_office_ltsc:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_365:*:*:*:*:*	CWE-200

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 zero-day vulnerability (CVE-2023-20588) affecting AMD processors. Apply the provided patch to mitigate the risk of speculative data disclosure on vulnerable systems.



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	<u>T1036</u> Masquerading	

Patch Details

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-20588>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36019>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-35630>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-35641>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-35628>

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-35636>

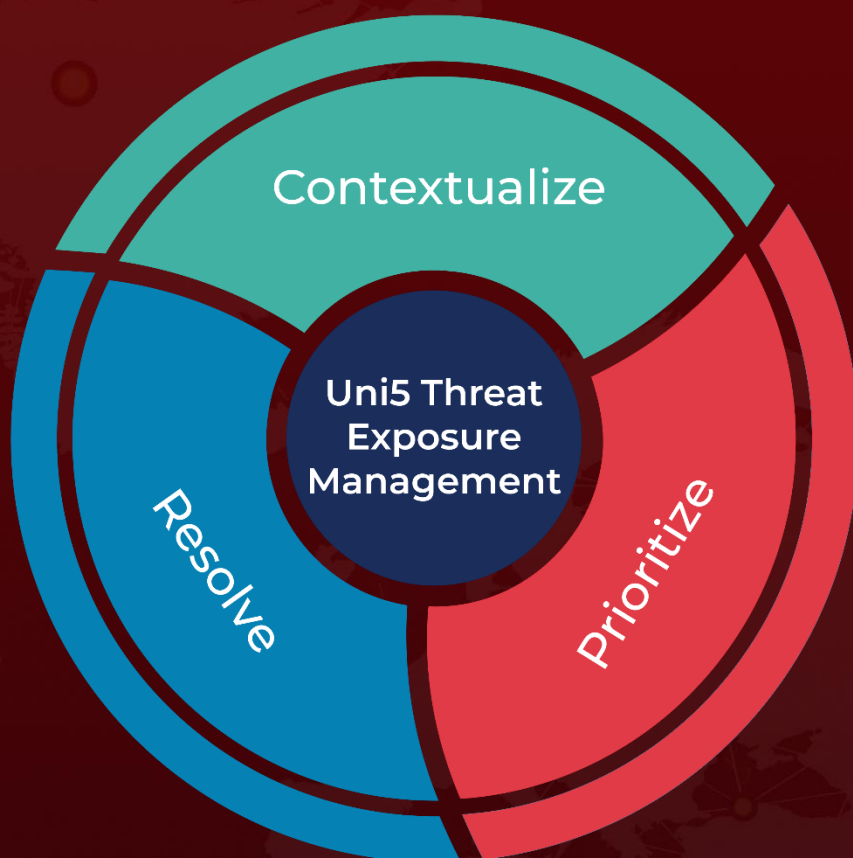
References

<https://msrc.microsoft.com/update-guide/releaseNote/2023-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 13, 2023 • 5:30 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com