Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's September 2023 Patch Tuesday Addresses Two Zero-day Vulnerabilities

Date of Publication	Admiralty Code	TA Number
September 13, 2023	A1	TA2023369

Summary

First Seen: September 12, 2023
Affected Platforms: Microsoft Exchange Server, Microsoft Word, Microsoft Streaming Service, Windows GDI, Windows Kernel, Windows Common Log File System Driver, Internet Connection Sharing (ICS), DHCP Server Service, Windows TCP/IP Information
Impact: Remote Code Execution, Security Feature Bypass, Information Disclosure, and Privilege Escalation, Denial of Service, Spoofing

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-36744	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-36745	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-36756	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-36761	Microsoft Word Information Disclosure Vulnerability	Microsoft Word	✓	✓	✓
CVE-2023-36777	Microsoft Exchange Server Information Disclosure Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-36802	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability	Microsoft Streaming Service	✓	✓	✓
CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability	Windows GDI	✗	✗	✓
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	✗	✗	✓
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	✗	✗	✓
CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-38148	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability	Internet Connection Sharing (ICS)	✗	✗	✓
CVE-2023-38152	DHCP Server Service Information Disclosure Vulnerability	DHCP Server Service	✗	✗	✓
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability	Windows TCP/IP Information	✗	✗	✓
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability	Windows GDI	✗	✗	✓

Vulnerability Details

#1

Microsoft's September 2023 Patch Tuesday includes security updates for 59 flaws, with two zero-day vulnerabilities actively exploited. Among these flaws, five are rated 'Critical,' including four remote code execution issues and an Azure Kubernetes Service elevation of privilege vulnerability. The breakdown of vulnerabilities includes 3 Security Feature Bypass, 24 Remote Code Execution, 9 Information Disclosure, 3 Denial of Service, and 5 Spoofing vulnerabilities. Additionally, 5 vulnerabilities in Microsoft Edge (Chromium) and 2 non-Microsoft flaws in Electron and Autodesk were addressed. This advisory pertains to 14 CVEs that hold considerable potential for exploitation.

#2

One of the actively exploited zero-day vulnerability is CVE-2023-36802, Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability, allowing attackers to gain SYSTEM privileges and it is rated important and has a CVSSv3 score of 7.8. It was discovered by multiple security researchers and was actively exploited.

#3

Another zero-day vulnerability is CVE-2023-36761, Microsoft Word Information Disclosure Vulnerability, which could steal NTLM hashes when opening a document, including in the preview pane and it is also rated important and has a CVSSv3 score of 6.2. This vulnerability was discovered internally by the Microsoft Threat Intelligence group, and it has been exploited in the wild as a zero-day.

#4

Microsoft warns that previewing a specially crafted file in the preview pane can trigger the exploit, potentially leading to the disclosure of NTLM hashes, which could be used in NTLM relay or pass-the-hash attacks. This marks the second zero-day vulnerability in 2023 that could result in NTLM hash disclosure.

#5

Both vulnerabilities are considered significant and have been exploited before a patch was available. 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-2023-36744	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:-:*:*:*:*:*:*	CWE-264
CVE-2023-36745		cpe:2.3:a:microsoft:microsoft_exchange_server:-:*:*:*:*:*:*	CWE-502
CVE-2023-36756		cpe:2.3:a:microsoft:microsoft_exchange_server:-:*:*:*:*:*:*	CWE-264
CVE-2023-36761	Microsoft Office: 365 - 2019 Microsoft Word: before 16.0.5413.1000 Microsoft 365 Apps for Enterprise: before 16.0.5413.1000	cpe:2.3:a:microsoft:microsoft_word:-:*:*:*:*:*:*	CWE-200
CVE-2023-36777	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:-:*:*:*:*:*:*	CWE-200

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-36802	Windows: 10 - 11 22H2 Windows Server: 2019 - 2022 20H2	cpe:2.3:a:microsoft:microsoft_streaming_service:-:*:*:*:*:*:*	CWE-119
CVE-2023-36804	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:a:microsoft:microsoft_windows_gdi:-:*:*:*:*:*:*	CWE-264
CVE-2023-38142	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:a:microsoft:microsoft_streaming_service:-:*:*:*:*:*:*	CWE-264
CVE-2023-38143	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H	cpe:2.3:a:microsoft:microsoft_windows_common_log_file_system_driver:-:*:*:*:*:*:*	CWE-264
CVE-2023-38144	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:a:microsoft:microsoft_windows_common_log_file_system_driver:-:*:*:*:*:*:*	CWE-264
CVE-2023-38148	Windows Server: 2019 - 2022 20H2 Windows: 10 - 11 22H2	cpe:2.3:a:microsoft:microsoft_internet_connection_sharing:-:*:*:*:*:*:*	CWE-20
CVE-2023-38152	Windows Server: 2008 - 2022 20H2	cpe:2.3:a:microsoft:microsoft_dhcp_server_service:-:*:*:*:*:*:*	CWE-200
CVE-2023-38160	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:a:microsoft:microsoft_windows_tcpip_information:-:*:*:*:*:*:*	CWE-264
CVE-2023-38161	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:a:microsoft:microsoft_windows_gdi:-:*:*:*:*:*:*	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 other 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.

Exercise meticulous surveillance on any security-related events that occur within devices and applications. If any abnormalities are discovered, take prompt action to begin the incident management procedure.

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

TA0040 Impact	**TA0042** Resource Development	**TA0007** Discovery	**TA0002** Execution
TA0003 Persistence	**TA0004** Privilege Escalation	**T1588** Obtain Capabilities	**T1588.005** Exploits
T1059 Command and Scripting Interpreter	**T1588.006** Vulnerabilities	**T1068** Exploitation for Privilege Escalation	**T1203** Exploitation for Client Execution
T1082 System Information Discovery			

Patch Details

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36744

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36745

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36756

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36761

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36777

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36802

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36804

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38142

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38143

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38144

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38148

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38152

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38160

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38161

References

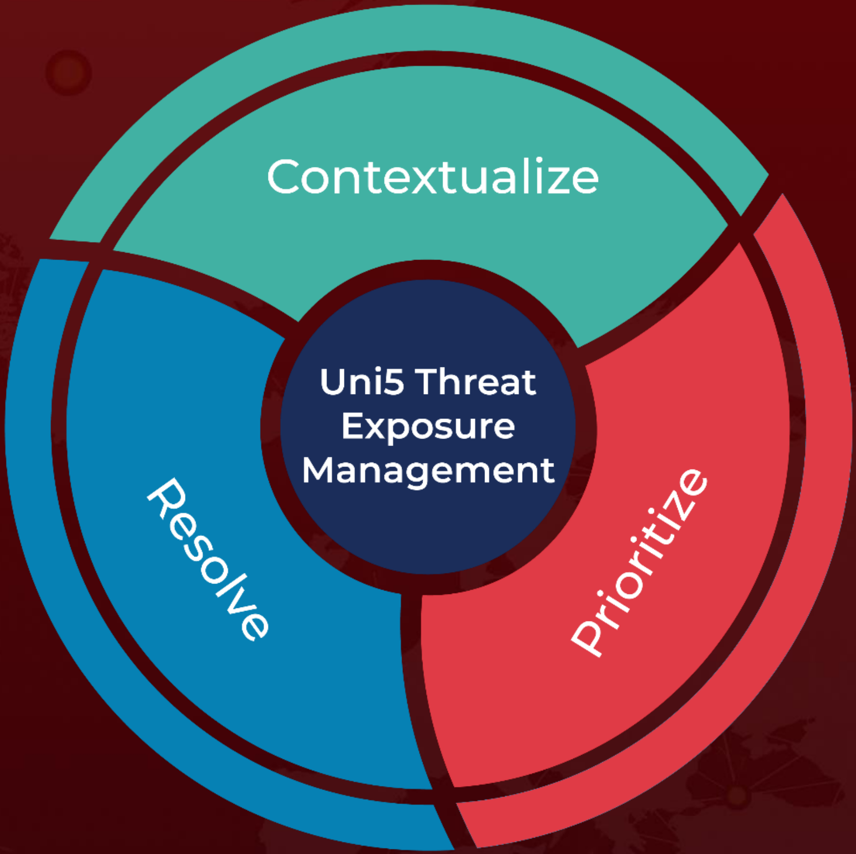
https://msrc.microsoft.com/update-guide/releaseNote/2023-Sep

https://www.cisa.gov/news-events/alerts/2023/09/12/microsoft-releases-september-2023-updates

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

September 13, 2023 • 7:30 AM

More at www.hivepro.com