Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's October 2023 Patch Tuesday Addresses Three Zero-day Vulnerabilities

Date of Publication	Admiralty Code	TA Number
October 11, 2023	A1	TA2023410

Summary

First Seen: October 11, 2023
Affected Platforms: Microsoft Skype for Business, Microsoft WordPad, Microsoft Message Queuing, Microsoft Virtual Trusted Platform Module, Microsoft Common Data Model SDK, Microsoft .Net, Microsoft ASP.NET Core, Windows IIS Server, Microsoft Office, Microsoft Windows
Impact: Privilege Escalation, Remote Code Execution, Information Disclosure, and, Denial of Service

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-41763	Microsoft Skype for Business Privilege Escalation Vulnerability	Microsoft Skype for Business	✓	✓	✓
CVE-2023-36563	Microsoft WordPad Information Disclosure Vulnerability	Microsoft WordPad	✓	✓	✓
CVE-2023-44487	HTTP/2 Rapid Reset Attack Vulnerability	Microsoft .Net, Microsoft ASP.NET Core, Microsoft Windows	✓	✓	✓
CVE-2023-35349	Microsoft Message Queuing Remote Code Execution Vulnerability	Microsoft Message Queuing	✗	✗	✓
CVE-2023-36697	Microsoft Message Queuing Remote Code Execution Vulnerability	Microsoft Message Queuing	✗	✗	✓
CVE-2023-36718	Microsoft Virtual Trusted Platform Module Remote Code Execution Vulnerability	Microsoft Virtual Trusted Platform Module	✗	✗	✓
CVE-2023-36566	Microsoft Common Data Model SDK Denial of Service Vulnerability	Microsoft Common Data Model SDK	✗	✗	✓
CVE-2023-36434	Windows IIS Server Elevation of Privilege Vulnerability	Windows IIS Server	✗	✗	✓
CVE-2023-36569	Microsoft Office Elevation of Privilege Vulnerability	Microsoft Office	✗	✗	✓

Vulnerability Details

#1

Microsoft's October 2023 Patch Tuesday includes security updates for 103 flaws, with three zero-day vulnerabilities actively exploited. Among these flaws, twelve are rated 'Critical,' while the remaining 91 are rated as 'Important.' The breakdown of vulnerabilities includes 3 Security Feature Bypass, 45 Remote Code Execution, 26 Elevation of Privilege, 12 Information Disclosure, 17 Denial of Service, and 1 Spoofing vulnerabilities.

#2

In addition, a Chromium vulnerability was fixed by Google on October 3rd and ported to Microsoft Edge. 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-2023-41763 is an Elevation of Privilege Vulnerability in Skype for Business, allowing potential breaches of internal networks. CVE-2023-36563 is an Information Disclosure Vulnerability in Microsoft WordPad, permitting the theft of NTLM hashes when opening documents. CVE-2023-44487 is an HTTP/2 Rapid Reset Attack, a zero-day DDoS attack technique actively exploited since August. It leveraged the stream cancellation feature in HTTP/2 to overwhelm target servers, creating a denial of service state.

#4

Microsoft has issued updates to address these issues and recommends applying them promptly to secure systems. It's also important to note that Windows Server 2012 and 2012 R2 reached end of life in October 2023, meaning they will no longer receive security updates.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-41763	Skype for Business Server: before 7.0.246.530	cpe:2.3:a:microsoft:skype_for_business_server:*:*:*:*:*:*:*:*:*	CWE-200

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-36563	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	CWE-200
CVE-2023-44487	ASP.NET Core: before 7.0.12 .NET: 6.0.0 - 7.0.11	cpe:2.3:a:microsoft:asp.net_core:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:.net:6.0.22:*:*:*:*:*:*:*	CWE-400
CVE-2023-35349	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	CWE-20
CVE-2023-36697	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	CWE-20
CVE-2023-36718	Windows: 10 - 11 22H2 Windows Server: 2016 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	CWE-20
CVE-2023-36566	Common Data Model SDK for TypeScript: before 1.7.4 Common Data Model SDK for Python: before 1.7.4 Common Data Model SDK for Java: before 1.7.4 Common Data Model SDK for C#: before 1.7.4	cpe:2.3:a:microsoft:common_data_model_sdk_for_typescript:*:*:*:*:*:*:*:*	CWE-20
CVE-2023-36434	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2 Microsoft IIS: 10.0	cpe:2.3:o:microsoft:windows:11:21H2:*:*:*:*:*:*	CWE-264
CVE-2023-36569	Microsoft Office: 2019 Microsoft Office LTSC 2021: All versions Microsoft 365 Apps for Enterprise: All versions	cpe:2.3:a:microsoft:microsoft_office:2019:*:*:*:*:*:*:*	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.

Don't neglect the non-security updates, including cumulative updates for Windows 11 and Windows 10. These updates may include performance improvements, stability fixes, and other important enhancements for your systems.

Windows Server 2012 and Windows Server 2012 R2 have reached end of support, meaning they won't receive security updates. Continuing to use these products poses a risk to your infrastructure. It's crucial for organizations to plan an upgrade.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	**TA0042** Resource Development	**TA0007** Discovery	**TA0002** Execution
TA0003 Persistence	**TA0040** Impact	**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	**T1498** Network Denial of Service		

Patch Details

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-41763

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36563

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-44487

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-35349

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36697

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36718

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36566

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36434

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36569

References

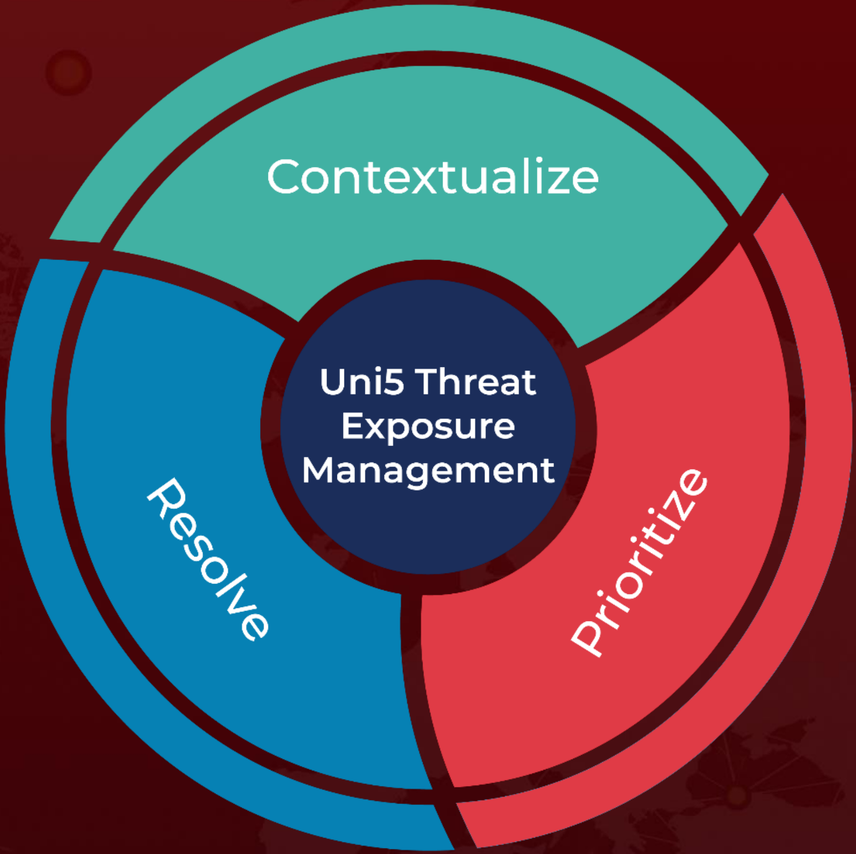
https://msrc.microsoft.com/update-guide/releaseNote/2023-Oct

https://www.cisa.gov/news-events/alerts/2023/10/10/microsoft-releases-october-2023-security-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

October 11, 2023 • 7:00 AM

More at www.hivepro.com