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 9 , 2023	A1	TA2023327

Summary

First Seen: August 8, 2023
Affected Products: Microsoft Exchange Server, Microsoft Office, and Windows
Impact: In the August Patch Tuesday release, Microsoft addressed a total of 73 CVEs, encompassing six critical and 67 important vulnerabilities. Within this range of vulnerabilities, the security update covered the typical spectrum of issues, including remote code execution (RCE) flaws, concerns related to privilege escalation, vulnerable security bypass mechanisms, and instances that facilitate information disclosure or trigger denial-of-service conditions. This advisory pertains to 15 CVEs that hold considerable potential for exploitation.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-35388	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-38182	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-38185	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-38180	.NET and Visual Studio Denial of Service Vulnerability	Microsoft .NET Core and Visual Studio	✓	✓	✓
CVE-2023-36884	Microsoft Office and Windows HTML Remote Code Execution Vulnerability	Microsoft Office and Windows	✓	✓	✓
CVE-2023-36910	Microsoft Message Queuing Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-36911	Microsoft Message Queuing Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2023-35385	Microsoft Message Queuing Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2023-35359	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2023-35380	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2023-35382	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2023-35386	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2023-21709	Microsoft Exchange Server Elevation of Privilege Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-35368	Microsoft Exchange Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-38154	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓

Vulnerability Details

#1

In the latest Patch Tuesday release for August, Microsoft addressed a total of 73 Common Vulnerabilities and Exposures (CVEs). Among these, six were assigned a critical rating, signifying their utmost severity, while the remaining 67 were deemed important due to their potential impact.

#2 Of particular note is CVE-2023-36884, a vulnerability that enabled malicious actors to meticulously craft Microsoft Office documents capable of circumventing the Mark of the Web (MoTW) security feature. This manipulation permitted the opening of files without triggering a security alert, thereby facilitating remote code execution. This vulnerability was actively exploited by a hacking group known as RomCom.

#3 Another significant concern is CVE-2023-38180, which involves a Denial of Service (DoS) vulnerability present in both .NET applications and Visual Studio. This vulnerability has been actively exploited, leading to potential DoS attacks that target systems running these applications.

#4 Additionally, CVE-2023-35385, CVE-2023-36910, and CVE-2023-36911 represent Remote Code Execution (RCE) vulnerabilities within the Microsoft Message Queuing (MSMQ) component of Windows. These vulnerabilities can be exploited by sending malicious MSMQ packets to a vulnerable server, potentially resulting in arbitrary code execution. Exploiting this flaw necessitates the active Message Queuing service on the server.

#5 Lastly, CVE-2023-21709 is an Escalation of Privileges (EoP) vulnerability in Microsoft Exchange Server. Unauthorized attackers attempting to guess passwords for valid accounts could exploit this flaw to impersonate users, thereby presenting a significant security risk.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-35388	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-20
CVE-2023-21709	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-2023-35368	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-20
CVE-2023-38154	Windows: 10 - 11 22H2, Windows Server: 2019 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	CWE-264

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-38182	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-20
CVE-2023-38185			
CVE-2023-38180	.NET: 6.0.0 - 7.0.9, Visual Studio: 17.2.0 17.2.32505.173 - 17.6.5 17.6.33829.357, ASP.NET Core: before 2.1.40	cpe:2.3:a:microsoft:.net:-:*:*:*:*:*:*:*	CWE-20
CVE-2023-36884	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2, Microsoft Office: 2013 – 2019, Microsoft Word: 2013 Service Pack 1 – 2019	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-20
CVE-2023-36910	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	CWE-20
CVE-2023-36911	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	CWE-20
CVE-2023-35385	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	CWE-20
CVE-2023-35359	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	CWE-264
CVE-2023-35380	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	CWE-264
CVE-2023-35382	Windows: 10 - 11 22H2, Windows Server: 2019 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	CWE-264
CVE-2023-35386	Windows: 10 - 11 22H2, Windows Server: 2016 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	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

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0040 Impact	**T1203** Exploitation for Client Execution	**T1059** Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1588.005** Exploits	**T1040** Network Sniffing
T1005 Data from Local System	**T1036** Masquerading	**T1574** Hijack Execution Flow	**T1211** Exploitation for Defense Evasion

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35388

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38182

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38185

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-36910

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-35385

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-35382

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-35386

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21709

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35368

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-38154

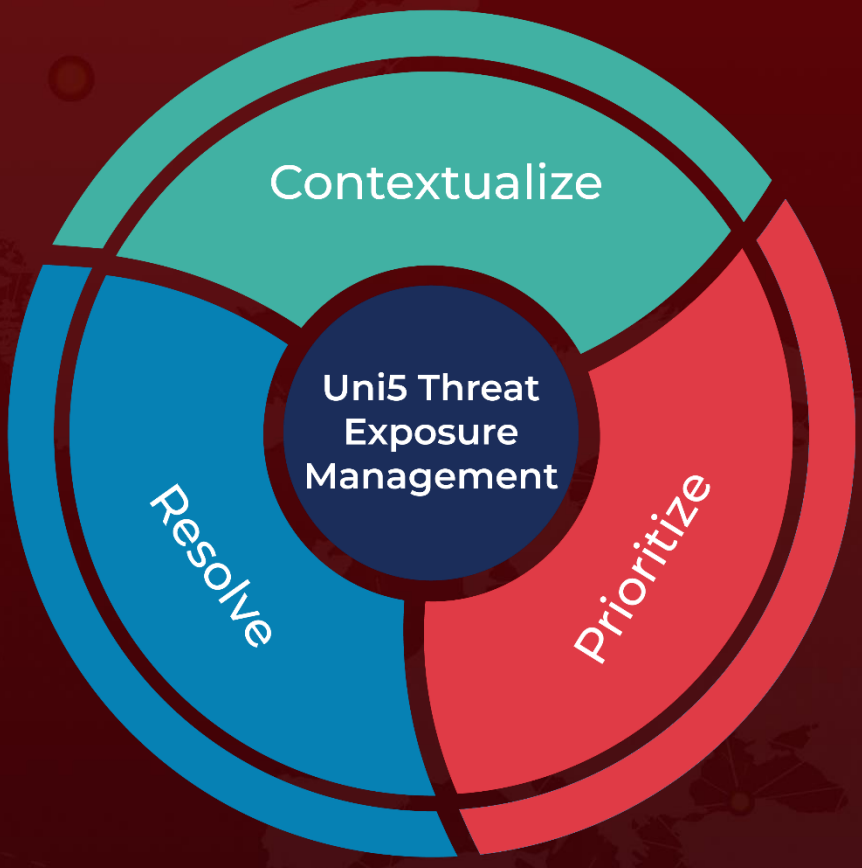
References

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

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 9, 2023 . 9:00 AM

More at www.hivepro.com