Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's June 2023 Patch Tuesday Addresses 78 Vulnerabilities

Date of Publication	Admiralty Code	TA Number
June 14, 2023	A1	TA2023262

Summary

First Seen: June 13, 2023
Affected Platforms: Microsoft Office SharePoint, Visual Studio, Windows Hyper-V, Windows PGM, Microsoft Exchange Server
Impact: Remote Code Execution, Denial of Service and Privilege Escalation

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-24897	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	.NET and Visual Studio	✗	✗	✓
CVE-2023-29357	Microsoft SharePoint Server Elevation of Privilege Vulnerability	Microsoft Office SharePoint	✗	✗	✓
CVE-2023-32013	Windows Hyper-V Denial of Service Vulnerability	Windows Hyper-V	✗	✗	✓
CVE-2023-29363	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	Windows PGM	✗	✗	✓
CVE-2023-32014	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	Windows PGM	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-32015	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	Windows PGM	✗	✗	✓
CVE-2023-28310	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-32031	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2023-29362	Remote Desktop Client Remote Code Execution Vulnerability	Remote Desktop Client	✗	✗	✓

Vulnerability Details

#1

Microsoft's June 2023 Patch Tuesday includes security updates for a total of 78 flaws, with 38 of them being remote code execution vulnerabilities. Out of the 78 flaws, only six are classified as 'Critical,' encompassing denial of service attacks, remote code execution, and privilege elevation.

#2

The vulnerabilities cover various Microsoft products such as Windows, Office, Exchange Server, Microsoft Edge (Chromium-based), SharePoint Server, .NET and Visual Studio, Microsoft Teams, Azure DevOps, Microsoft Dynamics, and the Remote Desktop Client.

#3

While no zero-day vulnerabilities or actively exploited bugs were patched on this occasion, there were notable vulnerabilities that were fixed. One of them was CVE-2023-29357, an elevation of privilege vulnerability in Microsoft SharePoint Server. This flaw could allow attackers to gain the privileges of other users, including administrators, by exploiting spoofed JWT authentication tokens.

#4

Another significant vulnerability was CVE-2023-32031, a remote code execution vulnerability in Microsoft Exchange Server. This flaw allowed authenticated attackers to execute malicious code on the server accounts through a network call.

#5

Additionally, Microsoft released updates for Microsoft Office, addressing vulnerabilities that could enable threat actors to execute remote code through maliciously crafted Excel and OneNote documents. These flaws required user interaction, such as clicking on a link in a malicious file or email. Microsoft also published several non-Microsoft CVEs, including five vulnerabilities for GitHub and three vulnerabilities for AutoDesk.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-24897	Visual Studio: 2013 Update 5 - 2022 version 17.6 Microsoft .NET Framework: 3.5 - 4.8.1 .NET: 6.0.0 - 7.0.0	cpe:2.3:a:microsoft:visual_studio:2013 Update 5:*:*:*:*:*:*:*	CWE-20
CVE-2023-29357	Microsoft SharePoint Server: 2019 - 2019	cpe:2.3:a:microsoft:microsoft_sharepoint_server:2019:*:*:*:*:*:*:*	CWE-264
CVE-2023-32013	Windows: 10 - 11 22H2 Windows Server: 2019 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	CWE-20
CVE-2023-29363	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	CWE-20
CVE-2023-32014			
CVE-2023-32015			

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-28310	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 CU13 2023H1:15.02.1258.012:*:*:*:*:*:*	CWE-20
CVE-2023-32031			
CVE-2023-29362	Windows: 10 - 11 22H2 Windows Server: 2008 R2 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	

Recommendations

Apply Security Patches: Immediately install the security patches released by Microsoft to address critical and high-severity vulnerabilities. Keep your software up to date by regularly checking for and applying the latest security updates and patches provided by the vendor.

Implement Least Privilege Principle: Follow the principle of least privilege by granting users the minimum permissions necessary to perform their tasks. This helps limit the impact of privilege escalation vulnerabilities, such as CVE-2023-29357 in Microsoft SharePoint Server, by reducing the privileges an attacker can assume if they gain unauthorized access.

Antivirus Software and Regular File Backup: Use up-to-date antivirus software to detect and block any potential threats. Regularly back up your important files to a secure location, so you can recover them if your system is compromised. Use strong and unique passwords for all your accounts and enable two-factor authentication whenever possible.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0007 Discovery	TA0002 Execution	TA0040 Impact
TA0003 Persistence	TA0004 Privilege Escalation	TA0008 Lateral Movement	T1068 Exploitation for Privilege Escalation
T1059 Command and Scripting Interpreter	T1210 Exploitation of Remote Services	T1021 Remote Services	T1018 Remote System Discovery
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1203 Exploitation for Client Execution

Patch Details

http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-24897

http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29357

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32013

http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29363

http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-32014

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32015

http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-28310

http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-32031

http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29362

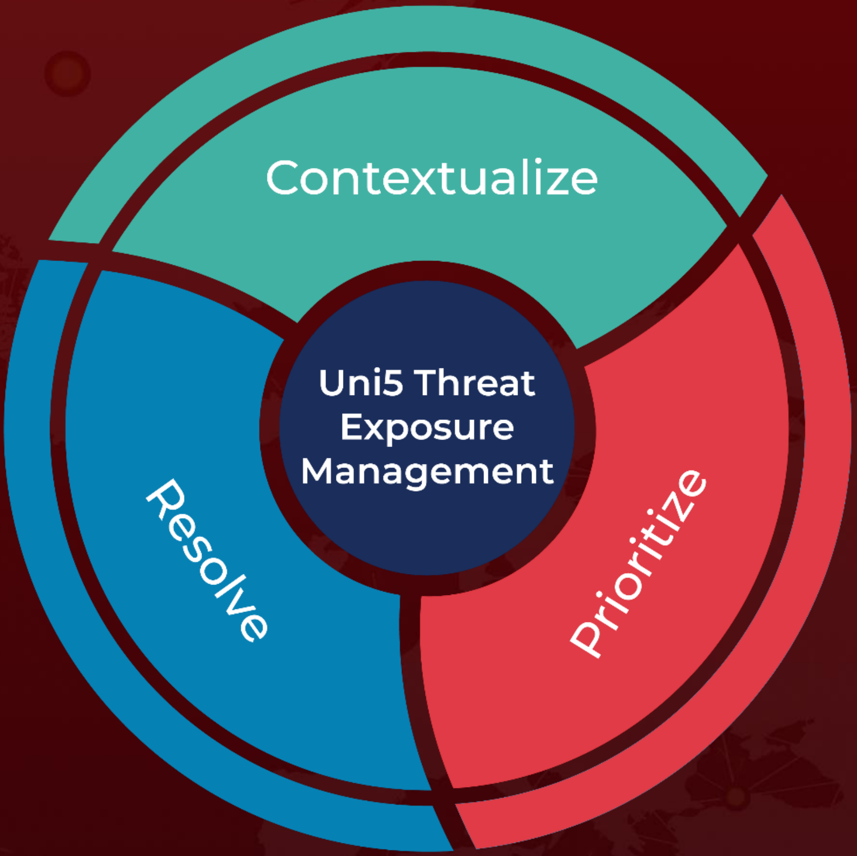
References

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

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

June 14, 2023 • 6:30 AM

More at www.hivepro.com