Hive Pro

THREAT ADVISORY

Microsoft addressed three zero-day vulnerabilities March 2022 Patch Tuesday Update

TA2022050

Threat Level RED

Publish Date –March 9, 2022

Microsoft addressed 71 the following vulnerabilities in their March 2022 Patch Tuesday Update. This advisory briefs about six vulnerabilities out of which three of them have been rated critical in severity and three of them are zero-days.

Microsoft Patch Tuesday comprise of following vulnerabilities:

- 29 Remote Code Execution Vulnerabilities
- 25 Elevation of Privilege Vulnerabilities
- 6 Information Disclosure Vulnerabilities
- 4 Denial of Service Vulnerabilities
- 3 Security Feature Bypass Vulnerabilities
- 3 Spoofing Vulnerabilities
- 1 Tampering Vulnerability

The three critical vulnerabilities are remote code execution bugs affecting Microsoft Exchange Server (CVE-2022-23277), HEVC Video Extensions (CVE-2022-22006), and VP9 Video Extensions (CVE-2022-24501). In addition to this, two out of the three zero-days are remote code execution (CVE-2022-24512 , CVE-2022-21990) and one of them is a privilege escalation (CVE-2022-24459). A zero-day vulnerability, CVE-2022-21990 has been labeled as "Exploitation More Likely" by Microsoft as a proof-of-concept (PoC) exploit is publicly available.

All these vulnerabilities have been patched by Microsoft and we advise all organizations to apply patches for the same to avoid potential attacks.

Potential Mitre ATT&CK TTPs are :
TA0001: Initial Access
TA0002: Execution
TA0004: Privilege Escalation
T1190: Exploit Public-Facing Application
T1203: Exploitation of Client Execution
T1068: Exploitation for Privilege Escalation

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-24512	Microsoft .NET Core: 3.1 Visual Studio: 2019 version 16.0 - 2022 version 17.0 .NET: 5.0 - 6.0	cpe:2.3:a:microsoft:microsoft_.net_core:3.1:*:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:.net:*:*:*:*:*:*:*:*	.NET and Visual Studio Remote Code Execution Vulnerability	CWE-94

Hive Pro

THREAT ADVISORY

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-21990	Windows: 7 - RT 8.1 Windows Server: 2008 - 2022	cpe:2.3:o:microsoft:windows_7:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_11:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008_r2:sp1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:sp2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012_r2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:*:*:*	Remote Desktop Client Remote Code Execution Vulnerability	CWE-94
CVE-2022-24459			Windows Fax and Scan Service Elevation of Privilege Vulnerability	CWE-264
CVE-2022-23277	Microsoft Exchange Server: 2013 - 2013 Service Pack 1, 2016 - 2016 Cumulative Update 22, 2019 - 2019 Cumulative Update 11	cpe:2.3:a:microsoft:microsoft_exchange_server:*:*:*:*:*:*:*:*	Microsoft Exchange Server Remote Code Execution Vulnerability	CWE-94
CVE-2022-22006	HEVC Video Extensions: All versions	cpe:2.3:a:microsoft:hevc_video_extensions:*:*:*:*:*:*:*:*	HEVC Video Extensions Remote Code Execution Vulnerability	CWE-94
CVE-2022-24501	VP9 Video Extensions: All versions	cpe:2.3:a:microsoft:vp9_video_extensions:*:*:*:*:*:*:*:*	VP9 Video Extensions Remote Code Execution Vulnerability	CWE-94

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24512
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21990
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24459
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23277
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22006
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24501

References

https://msrc.microsoft.com/update-guide/releaseNote/2022-Mar
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/08/microsoft-releases-march-2022-security-updates
https://msrc.microsoft.com/update-guide/en-us