Hive Pro

THREAT ADVISORY

Microsoft Patch Tuesday addresses a zero-day vulnerability in Windows Kernel	TA2022025

Threat Level	AMBER	Publish Date – Feb 9, 2022

Microsoft addressed 51 vulnerabilities in the February 2022 patch Tuesday release, one of which was classified as a zero-day vulnerability. A remote attacker could exploit some of these vulnerabilities to gain control of a vulnerable system. These vulnerabilities affect multiple products such as Microsoft excel, Azure Data Explorer, Teams, SQL server.

Out of the 51 flaws, 50 of them are rated important while one of them is rated moderate making it one of the few patch Tuesdays to not fix any critical vulnerabilities. Microsoft also addressed 19 chromium-based flaws in Microsoft edge which was assigned by Google.

The publicly disclosed zero-day bug has been assigned CVE-2022-21989 and has not been confirmed exploited in the wild. An attacker requires to take additional actions prior to exploitation to prepare the target environment for the successful exploitation of this vulnerability

Potential Mitre ATT&CK TTPs are :
TA0004: Privilege Escalation
T1068: Exploitation for Privilege Escalation

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-21989	Microsoft Windows 7 SP1, 8.1, 10, 10 20H2, 10 21H1, 10 21H2, 10 1607, 10 1809, 10 1909, 11, RT 8.1, Server 20H2, Server 2008 R2 SP1, Server 2008 SP2, Server 2012, Server 2012 R2, Server 2016, Server 2019, Server 2022, Server 2022 Azure Edition Core Hotpatch	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:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2022_azure_edition_core_hotpatch:*:*:*:*:*:*:*:*	Windows Kernel Elevation of Privilege Vulnerability	CWE-269

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21989

References

https://msrc.microsoft.com/update-guide/releaseNote/2022-Feb
https://thehackernews.com/2022/02/microsoft-and-other-major-software.html
https://www.zerodayinitiative.com/blog/2022/2/8/the-february-2022-security-update-review