Hive Pro

THREAT ADVISORY

Microsoft could not patch this vulnerability

TA202150

Threat Level RED

Publish Date – Nov 23, 2021

Microsoft released patches for 44 vulnerabilities on November 9th. CVE-2021-41379 was among them. However, installing this patch does not completely eliminate the vulnerability.

An exploit for a new Windows zero-day local privilege elevation vulnerability that grants admin privileges in Windows 10, Windows 11, and Windows Server has been publicly disclosed by a security researcher, Abdelhamid Naceri.

CVE-2021-41379 is a privilege escalation vulnerability that allows an attacker with limited access on a compromised system to move laterally within the same network. All the versions of Windows 10, Windows 11 and Windows server are affected by this vulnerability.

After examining Microsoft's fix,, the security researcher who discovered this vulnerability, discovered a bypass of the patch as well as a more powerful new zero-day privilege elevation vulnerability.

There are currently no workarounds for this vulnerability. Any attempt to directly patch the binary will result in a failure of the Windows installer. We must wait for Microsoft to resolve this issue.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-41379	Microsoft Windows 7SP1, 8.1, 10, 10 20H2, 10 21H1, 10 1607, 10 1809, 10 1909, 10 2004, 11, RT 8.1, Server 20H2, Server 2004, Server 2008 R2 SP1,Server 2008 SP2,Server 2012,Server 2012 R2,Server 2016,Server 2019,Server 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_10:1607:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*:*, 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:2004:*:*:*:*:*:*:*:*, 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:*:*:*:*:*:*:*:*	Windows Installer Elevation of Privilege Vulnerability	CWE-269

References

https://www.bleepingcomputer.com/news/microsoft/new-windows-zero-day-with-public-exploit-lets-you-become-an-admin/
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-41379