Hive Pro

THREAT ADVISORY

Microsoft could not patch this vulnerability yet again

TA202153

Threat Level AMBER

Publish Date – Nov 30, 2021

An improperly patched Windows vulnerability (CVE-2021-24084) can lead to local privilege escalation and information disclosure. The vulnerability was disclosed in October 2020 and even after Microsoft addressed this vulnerability in February 2021's Patch Tuesday, a researcher was able to exploit the patched vulnerability making it another zero-day made by improper patching.

CVE-2021-24084 was an information disclosure vulnerability in Windows Mobile Device Management component but later it was discovered that it could be exploited for local privilege escalation that allows an attacker to gain admin privilege and reading arbitrary files even if they don't have the permissions to do so. All the versions of Windows 10 even after the November patch are affected by this vulnerability.

After examining Microsoft's fix, Abdelhamid Naceri, 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. He also made the proof-of-concept available to the public.

An unofficial micro patch has been released by 0patch and will be available for free until Microsoft releases an official patch for the vulnerability.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-24084	Microsoft Windows, 10, 10 20H2, 10 21h1 , 10 1809, 10 1909, 10 2004	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_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*,	Windows Mobile Device Management Information Disclosure Vulnerability and Elevation of Privilege Vulnerability	CWE-269

Patch link

https://blog.0patch.com/2021/11/micropatching-unpatched-local-privilege.html

References

https://threatpost.com/unpatched-windows-zero-day-privileged-file-access/176609/
https://thehackernews.com/2021/11/unpatched-unauthorized-file-read.html
https://www.techradar.com/sg/news/nasty-windows-10-vulnerability-gets-a-patch-but-not-from-microsoft