

Windows 10 and 11 PC users need to update this patch immediately

Microsoft has released cumulative updates for Windows 10 and 11 PC systems via Patch Tuesday this month.

The latest Patch Tuesday patch released by Microsoft helps fix two Zero-day vulnerabilities and related evidence that these vulnerabilities have been exploited by hackers to launch a new attack. So users need to update them as soon as possible.



Both Windows 10 and 11 are vulnerable.

The first vulnerability tracking number is CVE-2024-26234. This is a proxy driver spoofing vulnerability that could use valid Microsoft hardware publishing certificates to certify malicious drivers. Sophos X-Ops is the security firm that discovered this vulnerability in December 2023 and team leader Christopher Budd reported this vulnerability to Microsoft.

According to the report, the malicious file labeled 'Category Customer Authentication Service' appears to impersonate Thales Group. Further investigation revealed that the malware also came with a marketing software called 'LaiXi Android Screen Mirroring'.

While Sophos could not verify the authenticity of the LaiXi software, Budd said it believes the file is a malicious backdoor.

Users are advised to update immediately.

Another vulnerability identified as CVE-2024-29988 can bypass system protection mechanisms and disable SmartScreen prompts. The vulnerability was discovered by Peter Girnus of Trend Micro's Zero-Day Project and Dmitrij Lenz and Vlad Stolyarov of Google's Threat Analysis Team.

Dustin Childs, director of threat intelligence at ZDI, pointed out that attackers could use this vulnerability to evade EDR/NDR detection and bypass Mark of the Web (MoTW) functionality. , and can deploy many types of malware on the target Windows system.

You finished reading the article "**Windows 10 and 11 PC users need to update this patch immediately**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.