Detects a vulnerability that threatens all Windows computers shipped from 2012 up to now

Security researchers have found a vulnerability in the Microsoft Windows Platform Binary Table (WPBT). This vulnerability can be exploited by hackers to install rootkits on all Windows computers shipped from 2012 to the present.

A rootkit is a type of malicious tool that hackers create silently to take full control of the victim's system. More dangerous, rootkits can hide deep in the operating system to avoid detection.

WPBT is the ACPI (Advanced Configuration and Power Interface) fixed firmware board introduced by Microsoft since Windows 8. Its mission is to allow vendors to execute programs every time the device boots.

However, besides allowing OEMs to forcibly install critical software that cannot be bundled with WINdows installation, this mechanism also allows hackers to deploy malicious tools. Microsoft itself has warned about this in their support documents.

Affects all computers running Windows 8 and above

This vulnerability was discovered by security researchers of Eclypsium. To exploit the vulnerability, hackers can use other techniques such as allowing writes to the memory where ACPI tables (including WPBT) are located or using a bootloader containing malicious code.

Hackers can successfully attack by abusing the BootHole vulnerability that allows Secure Boot bypass or DMA attacks from peripheral devices or other vulnerable components.

Here is a video demo of Eclypsium's attack:

Remedies

After receiving the notice from Eclypsium, Microsoft recommended that users use the Windows Defender Application Control (WADC) policy to control which binaries can run on Windows devices. WDAC policies can only be created on clients running Windows 10 version 1903 or later, Windows 11 or Windows Server 2016 or later.

On older Windows computers, you can use AppLocker policies to control what applications are allowed to run on the Windows client.

According to Eclypsium statistics, the issue affects 129 consumer and enterprise latpop, desktop and tablet models, including devices protected by Secure Boot and Dell Secured- core. It is estimated that about 30 million personal devices are at risk of being attacked by this vulnerability.