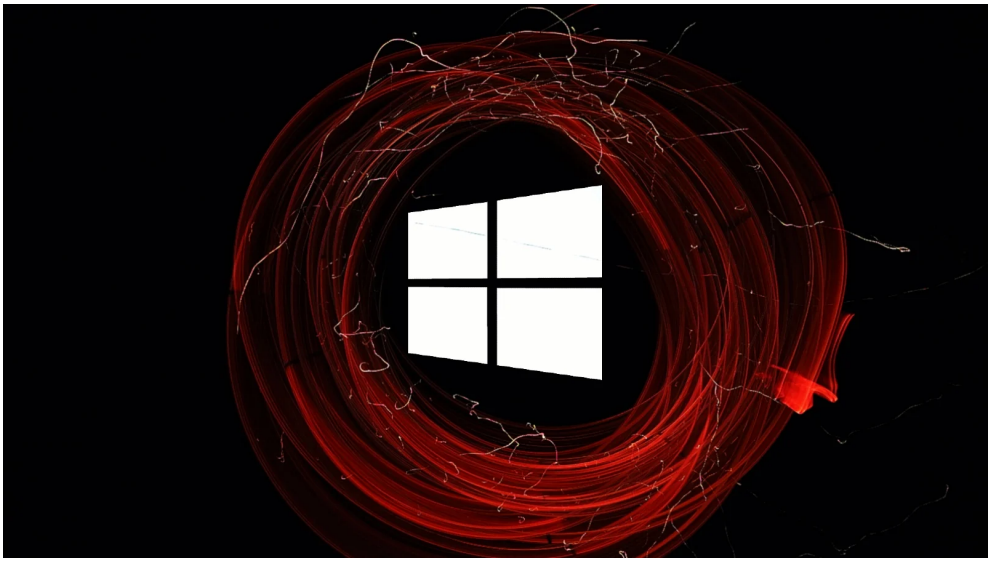
# Microsoft WPBT flaw lets hackers install rootkits on Windows devices

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** September 25, 2021 11:16 AM 1



Security researchers have found a flaw in the Microsoft Windows Platform Binary Table (WPBT) that could be exploited in easy attacks to install rootkits on all Windows computers shipped since 2012.

Rootkits (https://www.bleepingcomputer.com/tag/rootkit/) are malicious tools threat actors create to evade detection by burying deep into the OS and used to fully take over compromised systems while evading detection.

WPBT (https://download.microsoft.com/download/8/a/2/8a2fb72d-9b96-4e2d-a559-4a27cf905a80/windows-platform-binary-table.docx) is a fixed firmware ACPI (https://uefi.org/specs/ACPI/6.4/) (Advanced Configuration and Power Interface) table introduced by Microsoft starting with Windows 8 to allow vendors to execute programs every time a device boots.

However, besides enabling OEMs to force install critical software that can't be bundled with Windows installation media, this mechanism can also allow attackers to deploy malicious tools, as Microsoft warns in its own documentation.

"Because this feature provides the ability to persistently execute system software in the context of Windows, it becomes critical that WPBT-based solutions are as secure as possible and do not expose Windows users to exploitable conditions," Microsoft explains.

"In particular, WPBT solutions must not include malware (i.e., malicious software or unwanted software installed without adequate user consent)."

## Impacts all computers running Windows 8 or later

The weakness found by Eclypsium researchers is present on Windows computers since 2012, when the feature was first introduced with Windows 8.

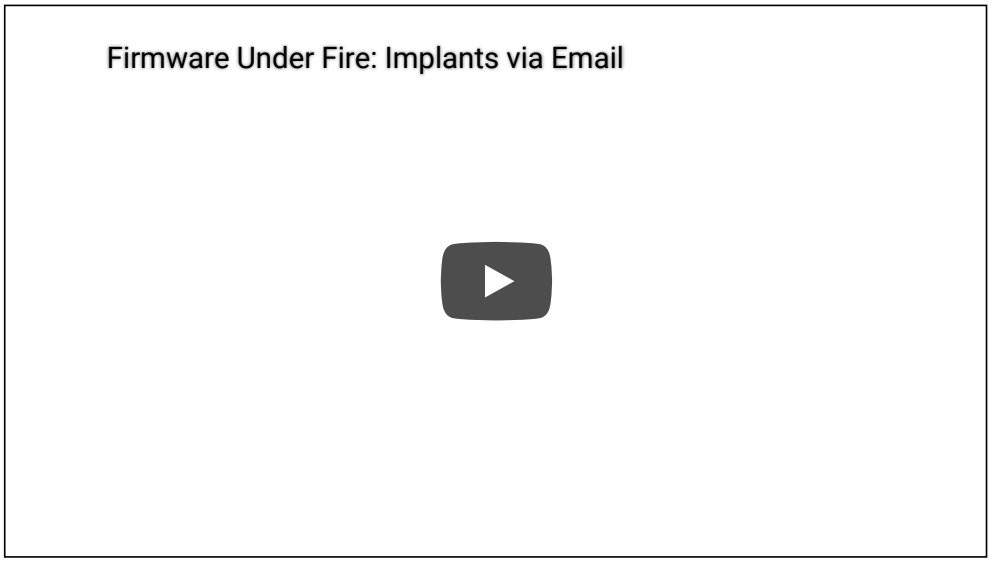
These attacks can use various techniques that allow writing to memory where ACPI tables (including WPBT) are located or by using a malicious bootloader.

This can be by abusing the BootHole (https://eclypsium.com/2020/08/21/securing-the-enterprise-from-boothole/) vulnerability that bypasses Secure Boot or via DMA attacks (https://eclypsium.com/2020/01/30/direct-memory-access-attacks/) from vulnerable peripherals or components.

"The Eclypsium research team has identified a weakness in Microsoft’s WPBT capability that can allow an attacker to run malicious code with kernel privileges when a device boots up," Eclypsium researchers said.

"This weakness can be potentially exploited via multiple vectors (e.g. physical access, remote, and supply chain) and by multiple techniques (e.g. malicious bootloader, DMA, etc)."

Eclypsium has shared the following demo video that demonstrates how this security flaw can be exploited.




## Mitigation measures include using WDAC policies

After Eclypsium informed Microsoft of the bug, the software giant recommended using a Windows Defender Application Control policy (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview) which allows controlling what binaries can run on a Windows device.

"WDAC policy is also enforced for binaries included in the WPBT and should mitigate this issue," Microsoft states in the support document.

WDAC policies can only be created on client editions of Windows 10 1903 and later and Windows 11 or on Windows Server 2016 and above.

On systems running older Windows releases, you can use AppLocker policies to control what apps are allowed to run on a Windows client.

"These motherboard-level flaws can obviate initiatives like Secured-core because of the ubiquitous usage of ACPI and WPBT," Eclypsium researchers added.

"Security professionals need to identify, verify and fortify the firmware used in their Windows systems. Organizations will need to consider these vectors, and employ a layered approach to security to ensure that all available fixes are applied and identify any potential compromises to devices."

Eclypsium found another vector of attack allowing threat actors to take control of a targeted device's boot process and break OS-level security controls in the BIOSConnect feature of Dell SupportAssist (https://www.bleepingcomputer.com/news/security/dell-supportassist-bugs-put-over-30-million-pcs-at-risk/), a software that comes preinstalled on most Dell Windows devices.

As the researchers revealed, the issue "affects 129 Dell models of consumer and business laptops, desktops, and tablets, including devices protected by Secure Boot and Dell Secured-core PCs," with roughly 30 million individual devices being exposed to attacks.

## Related Articles:

How to fix printers asking for admins creds after PrintNightmare patch (https://www.bleepingcomputer.com/news/microsoft/how-to-fix-printers-asking-for-admins-creds-after-printnightmare-patch/)

New Windows security updates break network printing (https://www.bleepingcomputer.com/news/security/new-windows-security-updates-break-network-printing/)

Windows 10 upgrades blocked by old CryptoPro CSP versions (https://www.bleepingcomputer.com/news/microsoft/windows-10-upgrades-blocked-by-old-cryptopro-csp-versions/)

New Windows PrintNightmare zero-days get free unofficial patch (https://www.bleepingcomputer.com/news/microsoft/new-windows-printnightmare-zero-days-get-free-unofficial-patch/)

Windows admins now can block external devices via layered Group Policy (https://www.bleepingcomputer.com/news/microsoft/windows-admins-now-can-block-external-devices-via-layered-group-policy/)