BlackX: a UEFI bootkit on fully patched Windows, and why “patched” is not the same as “revoked”

10 November 2026 · 5 min read · blogs.iictp.org/blackx-uefi-bootkit-secure-boot-revocation

Ars Technica reports that a UEFI bootkit called BlackX infected Windows machines that had every relevant update installed. It is a useful reminder that installing a patch and closing the hole are not always the same thing.

TL;DR The short version

- Ars Technica reports that a UEFI bootkit called BlackX infected Windows machines with every relevant update installed.
- As with BlackLotus in 2023, installing a patch is not the same as enforcing the Secure Boot revocations that close the hole.
- Treat 'patch installed' and 'protection enforced' as separate facts, and verify which revocation steps your fleet has actually completed.

Read online, listen to it, or change the text size: https://blogs.iictp.org/blackx-uefi-bootkit-secure-boot-revocation

The background

Ars recalls that in 2023 a bootkit called BlackLotus became the first publicly documented in-the-wild bootkit able to bypass Secure Boot on fully updated Windows 11. The bootkit runs before Windows fully loads, so many defences are not yet running. Microsoft had patched the underlying flaw in 2022, and in 2023 and 2024 shipped further updates: one added a certificate that stops trusting the vulnerable boot managers, and another provided the means to revoke trust in the certificate that signed older vulnerable boot managers.

What was reported

Ars reports that the organisations hit by BlackX had installed all of those updates and were still infected, and frames the story around Microsoft’s lack of clarity about what Secure Boot protections are actually in force.

What it means for practitioners

- Treat “patch installed” and “protection enforced” as two separate facts, and verify the second one.
- Ask which revocation steps are optional, which are staged, and which your fleet has actually completed.
- Measure the state of firmware and boot trust on endpoints, not only OS patch levels.
- Keep a recovery path for machines whose boot chain you cannot trust: reflash, re-image, replace.

The governance point is the durable one: a control you cannot observe is a control you cannot claim to have.

> Facts in this post were read from the sources listed below on 10 November 2026; this is a developing story or product and details may have changed since.

Sources and further reading

1. Ars Technica. UEFI bootkit infected fully patched Windows machines. Is Microsoft to blame? 3 November 2026. arstechnica.com/security/2026/11/uefi-bootkit-infected-fully-patched-windows-machines-is-microsoft-to-blame/

Published by IICTP, an independent technical credential body, on 10 November 2026. The current version of this post is at https://blogs.iictp.org/blackx-uefi-bootkit-secure-boot-revocation. More guides: blogs.iictp.org.