A critical flaw in EDK II firmware code: how to respond when the bug is below the operating system

10 November 2026 · 5 min read · blogs.iictp.org/edk2-uefi-firmware-flaw-servers

Ars Technica reported on 27 October on a critical vulnerability in TianoCore EDK II, the open-source codebase that hardware makers and cloud providers use to build the UEFI firmware that runs when a machine starts. The patching problem is different from a normal software flaw.

TL;DR The short version

- Ars Technica reported a critical flaw, rated 9.5 out of 10, in TianoCore EDK II, the open-source code behind most UEFI firmware.
- Firmware fixes travel from the code owner through firmware suppliers and hardware makers before reaching you, and often need a reboot.
- Keep an inventory of firmware versions and subscribe to your hardware and cloud providers' security advisories.

Read online, listen to it, or change the text size: https://blogs.iictp.org/edk2-uefi-firmware-flaw-servers

What was reported

- Ars gives the flaw a severity rating of 9.5 out of 10, tracked as CVE-2026-97631, and says it allows code execution early in the boot process.
- Ars says virtually all UEFI suppliers, including AMI, Insyde and Phoenix, use the EDK II reference code extensively, and that Microsoft’s hardened fork, Project Mu, also used the affected code.
- Ars describes the flaw as affecting boot-time firmware used by most of the world’s server vendors and data centres.

Why firmware patching is a different job

- The fix usually travels from the code owner to a firmware supplier, then to the hardware maker, then to you. Each step takes time and may stop.
- Applying it means a firmware update and often a reboot, on machines that may be hard to take offline.
- You may not know which firmware version each server runs unless you have measured it.

What to do

- Build an inventory of firmware versions across servers and workstations, if you do not have one.

- Subscribe to your hardware vendors' and cloud providers' security advisories, and note which of them have published guidance for this CVE.
- Plan rolling firmware updates the same way you plan OS patching: staged, with a rollback path.
- Where you use a cloud provider, ask what they have done at their layer, and what remains yours.
- Read this alongside BlackX: both are about trust in the boot chain.

> 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. Code-execution flaw in UEFI firmware affects most servers on planet Earth. 27 October 2026. arstechnica.com/security/2026/10/code-execution-flaw-in-uefi-firmware-threatens-most-servers-on-planet-earth/

Published by IICTP, an independent technical credential body, on 10 November 2026. The current version of this post is at https://blogs.iictp.org/edk2-uefi-firmware-flaw-servers. More guides: blogs.iictp.org.