Code-execution flaw in UEFI firmware affects most servers on planet Earth

Defenders across the world face the burden of responding to yet another botched code-execution vulnerability, this time in boot-time firmware used by most of the world's server vendors and data centers.

The vulnerability, with a severity rating of 9.5 out of 10, resides in the TianoCore EDK II, an open source codebase that hardware makers and cloud providers use to create the UEFI firmware that runs during the boot-up sequence. Last year, a representative of the UEFI Forum called EDK2 the "preeminent solution / implementation of the UEFI specifications." Virtually all UEFI suppliers (sometimes still called IBVs or independent BIOS vendors), including AMI, Insyde, and Phoenix, use the reference code extensively. Project Mu, Microsoft's hardened EDK2 fork, used the code containing the vulnerable component as well.

The vulnerability, tracked as CVE-2026-97631, is a memory-corruption flaw in an ICMP component that attackers can exploit to execute malicious code that runs before the operating system and firmware can implement defenses like Secure Boot, which establishes a chain of trust for all code, including the Trusted Platform Module (TPM), loaded during boot. While final payloads delivered by CVE-2026-97631 have no persistence—meaning they run only once—they can give attackers a wide opening to install other payloads that also run each time early in the boot process.

Read full article

Comments

https://arstechnica.com/security/2026/10/code-execution-flaw-in-uefi-firmware-threatens-most-servers-on-planet-earth/