Siemens SIMATIC IPCs: test key weakens UEFI Secure Boot (CVE-2026-72895)



CISA reports that a BIOS vendor test key in the UEFI Secure Boot database of several Siemens SIMATIC IPCs can let a local attacker bypass Secure Boot. Siemens has released fixed versions and advises updating.

- CVE-2026-72895 is a use of a default cryptographic key: a BIOS vendor test key sits in the Secure Boot key database.
- A local attacker with physical or administrative access could boot an operating system or UEFI application signed with that key, even with Secure Boot enabled.
- Affected: SIMATIC IPC BX-21A below 31.01.13, IPC RW-543A below 1.1.4, and IPC227G/277G/277G PRO/327G/377G below 28.01.15.
- The CVSS v3 score is 7.7.

> - Siemens has released new versions and recommends updating to the latest.

What was reported

CISA has published an advisory on several Siemens SIMATIC industrial PCs. A BIOS vendor test key is present in the UEFI Secure Boot key database (CVE-2026-72895, classed as use of a default cryptographic key). The CVSS v3 score is 7.7.

A local attacker with physical or administrative access to a device could use the key to boot an operating system or UEFI application signed with it. This bypasses UEFI Secure Boot protections even when Secure Boot is enabled.

Affected products

- SIMATIC IPC BX-21A: versions below 31.01.13
- SIMATIC IPC RW-543A: versions below 1.1.4
- SIMATIC IPC227G, IPC277G, IPC277G PRO, IPC327G and IPC377G: versions below 28.01.15

CISA lists the affected sectors as including critical manufacturing, transportation, energy, healthcare, financial services and government facilities, with deployment worldwide.

What to do next

Siemens has released new versions of the affected products and recommends updating to the latest ones. Because exploitation requires local physical or administrative access, institutions should first identify where these devices are installed, then schedule the update through normal change control. The advisory does not report exploitation in the wild.

What to do now

1. Inventory SIMATIC IPC BX-21A, RW-543A and IPC227G/277G/277G PRO/327G/377G devices and record their BIOS versions.
2. Schedule updates to the fixed versions Siemens has released, using change control and testing for operational environments.
3. Restrict physical access to affected devices and review who holds administrative rights on them.
4. Where updates must wait, document the exception and the compensating controls in the risk register.
5. Confirm after patching that the devices run the fixed versions.