Siemens PSS SINCAL: WibuKey Driver Flaw Can Crash Systems Using Dongle Licensing



CISA reports an out-of-bounds write flaw (CVE-2026-84854) in the WibuKey component used by Siemens PSS SINCAL, which can cause a denial of service. It affects only installations using the legacy WibuKey dongle licence.

- CVE-2026-84854 is an out-of-bounds write in the third-party WibuKey driver.
- Exploitation could crash the system and cause denial of service.
- Only PSS SINCAL configured with the legacy WibuKey dongle licence type is affected.
- Affected: V21.5 and V22.0 (all versions) and V22.5 before 22.5.5.
- Siemens is preparing updates and recommends mitigations where patches are not yet available.

CISA has published an advisory on Siemens PSS SINCAL concerning a vulnerability in WibuKey, a third-party product the software uses for licensing.

What is affected

The flaw, tracked as **CVE-2026-84854**, sits in the WibuKey driver. Insufficient validation of user input when calculating the size of a kernel buffer can lead to an out-of-bounds write. An attacker who exploits it could crash the system, resulting in a denial-of-service condition.

The issue matters only when PSS SINCAL is configured to use the legacy WibuKey dongle licence type. The affected versions are V21.5 (all versions), V22.0 (all versions) and V22.5 earlier than 22.5.5.

CISA lists the relevant sectors as including energy, transportation, financial services, healthcare, government services and critical manufacturing, with deployment worldwide. Siemens is headquartered in Germany.

Status of fixes

Siemens is preparing updates and recommends mitigations for products where patches are not yet available. The source does not detail the specific mitigations in the portion provided, so teams should consult the Siemens and CISA advisories directly.

What to do

Organisations that use PSS SINCAL for network planning and analysis should first establish whether any installation relies on the legacy dongle licence. If none does, the exposure described here does not apply. Where it does, plan the move to a fixed version and apply Siemens' interim guidance in the meantime.

What to do now

1. Inventory all PSS SINCAL installations and record version and licence type.
2. Identify any using the legacy WibuKey dongle licence, as only these are affected.
3. Upgrade V22.5 installations to 22.5.5 or later; plan upgrades for V21.5 and V22.0 as Siemens releases updates.
4. Apply Siemens' recommended mitigations where no patch is available yet.
5. Restrict access to workstations running affected installations to authorised users.
6. Track the Siemens advisory for update releases and record decisions in the risk register.