Siemens SIMATIC WinCC: database privilege escalation flaw (CVE-2026-59241)



CISA reports that SIMATIC WinCC V7.5, V8.0 and V8.1 contain a database privilege flaw (CVE-2026-59241, CVSS 8.8). Siemens advises updating and applying mitigations where no fix exists yet.

- CVE-2026-59241 is an incorrect privilege assignment flaw with a CVSS v3 score of 8.8.
- An authenticated user with database access could execute commands on the underlying host system.
- Affected: WinCC V7.5 (all versions), V8.0 before 8.0.0.11, and V8.1 before 8.1.7.
- Siemens has released new versions for several products and is preparing further fixes.
- Mitigations are recommended where fixes are not yet available.

What was reported

CISA has published an advisory on a vulnerability in several versions of Siemens SIMATIC WinCC. The application does not sufficiently restrict the permissions assigned to a database role. As a result, an authenticated user who has access to the database could run commands on the underlying host system. The issue is tracked as **CVE-2026-59241** and carries a CVSS v3 score of 8.8.

Affected versions and vendor response

The advisory lists SIMATIC WinCC V7.5 (all versions), V8.0 versions earlier than 8.0.0.11, and V8.1 versions earlier than 8.1.7. Siemens has released new versions for several of the affected products and recommends moving to the latest releases. Further fixes are in preparation, and Siemens recommends mitigations for products where a fix is not yet, or not, available.

CISA notes that the product is deployed worldwide and used in sectors including critical manufacturing, energy, transportation, healthcare, financial services and government facilities.

What to do next

Because exploitation requires an authenticated account with database access, the first priority is to know where WinCC runs and who can reach its database. Plan updates for the fixed versions, and for V7.5 follow the mitigations in the Siemens advisory until a fix is offered. Treat any changes to production control systems through your normal change and testing process.

What to do now

1. Inventory all SIMATIC WinCC installations and record their versions against the affected ranges.
2. Review which accounts hold database access on WinCC systems and remove any that are not needed.
3. Schedule updates to WinCC V8.0.0.11 or later and V8.1.7 or later, tested before production rollout.
4. For V7.5 and other products without a fix, apply the mitigations in the Siemens advisory.
5. Restrict network access to WinCC database services to authorised hosts only and monitor for unusual command execution.