Siemens RUGGEDCOM CROSSBOW SAC: SQLite Flaws Fixed in Version 6.0



CISA reports multiple SQLite vulnerabilities in Siemens RUGGEDCOM CROSSBOW Station Access Controller below version 6.0, with a CVSS v3 score of 9.8. Siemens advises updating to the latest version.

- Affected: RUGGEDCOM CROSSBOW Station Access Controller (SAC) versions below 6.0.
- Flaws sit in the integrated SQLite component and could allow code execution, denial of service or disclosure of sensitive information.
- Listed CVEs: CVE-2025-6965, CVE-2025-70873, CVE-2025-71316, CVE-2026-11822 and CVE-2026-11824.
- The advisory gives a CVSS v3 score of 9.8.
- Siemens has released a new version and recommends updating to the latest one.

What was reported

CISA has published an industrial control systems advisory on the Siemens RUGGEDCOM CROSSBOW Station Access Controller (SAC). The product includes an SQLite component that contains several vulnerabilities. According to the advisory, an attacker could exploit them to execute arbitrary code, cause a denial of service, or obtain sensitive information.

The advisory lists five CVEs: CVE-2025-6965, CVE-2025-70873, CVE-2025-71316, CVE-2026-11822 and CVE-2026-11824. The weakness types named include numeric truncation error, improper clearing of heap memory before release, improper handling of Unicode encoding, and heap-based buffer overflow. The vendor equipment CVSS v3 score is 9.8.

Who is affected

All SAC versions below 6.0 are affected. CISA notes the product is deployed worldwide and lists the sectors concerned as critical manufacturing, transportation systems, energy, healthcare and public health, financial services, and government services and facilities. Siemens is headquartered in Germany.

Recommended response

Siemens has released a new version and recommends moving to the latest release. Organisations should confirm whether the product is present in their environment, check the installed version, and plan the update through normal change control. The source does not describe exploitation in the wild, so prioritisation should rest on the severity score and on how exposed each deployment is.

What to do now

1. Check asset inventories for RUGGEDCOM CROSSBOW SAC and record the installed version.
2. Schedule an update to the latest Siemens version for any instance below 6.0.
3. Until patched, restrict network access to SAC systems to authorised management hosts only.
4. Review SAC logs for unexpected crashes or unusual database activity.
5. Record the exposure and remediation in the OT risk register and report per internal governance.