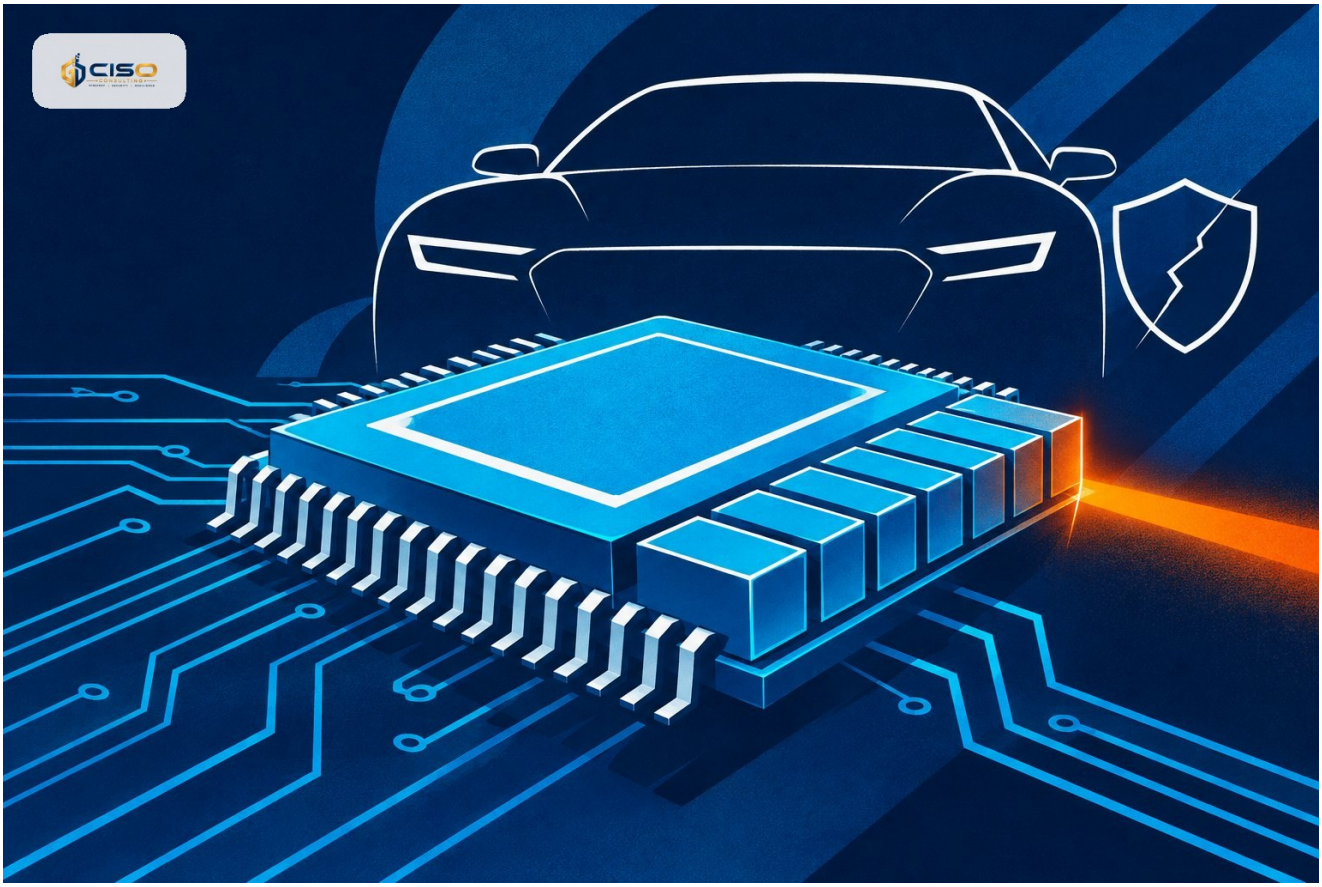
Siemens Capital Embedded AR Classic: out-of-bounds read flaw (CVE-2026-89208)



CISA reports an out-of-bounds read flaw, CVE-2026-89208 (CVSS v3 5.3), in Siemens Capital Embedded AR Classic. Siemens has released a fixed R20-11 version and is preparing further fixes.

- CVE-2026-89208 is an out-of-bounds read caused by missing input bounds validation when accessing packet data.
- Affected: Capital Embedded AR Classic 431-422 (all versions) and R20-11 versions below 2303.
- An unauthenticated remote attacker could cause abnormal behavior, instability or denial of service.
- CVSS v3 score is 5.3; Siemens recommends updating R20-11 to the latest version.
- Where no fix exists yet, Siemens recommends specific countermeasures.

What was reported

CISA has published an advisory on an out-of-bounds read vulnerability, tracked as CVE-2026-89208, in Siemens Capital Embedded AR Classic. The product does not properly validate input bounds before accessing packet data. An unauthenticated remote attacker could use this to cause abnormal product behavior, instability or denial of service. The advisory gives a CVSS v3 score of 5.3.

Affected versions and fixes

Two sets of versions are affected: Capital Embedded AR Classic 431-422 in all versions, and Capital Embedded AR Classic R20-11 in versions below 2303. Siemens has released a new version for R20-11 and recommends moving to the latest one. It is preparing further fix versions and advises specific countermeasures for products where a fix is not yet available.

The advisory lists critical manufacturing, transportation, energy, healthcare, financial services and government facilities among the sectors where the product is deployed, worldwide. Siemens is headquartered in Germany.

What to do

The rating is moderate, but the product is embedded software, so exposure may not be obvious from standard asset lists. Institutions should first confirm whether any device or supplier component they operate includes this software, then follow Siemens guidance on updates and countermeasures.

What to do now

1. Check asset inventories and ask suppliers whether devices contain Capital Embedded AR Classic 431-422 or R20-11.
2. Update R20-11 deployments below version 2303 to the latest Siemens release after testing.
3. For 431-422 and other unfixed products, apply the countermeasures in the Siemens advisory.
4. Track Siemens announcements for the further fix versions it is preparing.
5. Record the finding and remediation status in the OT and vulnerability management registers.