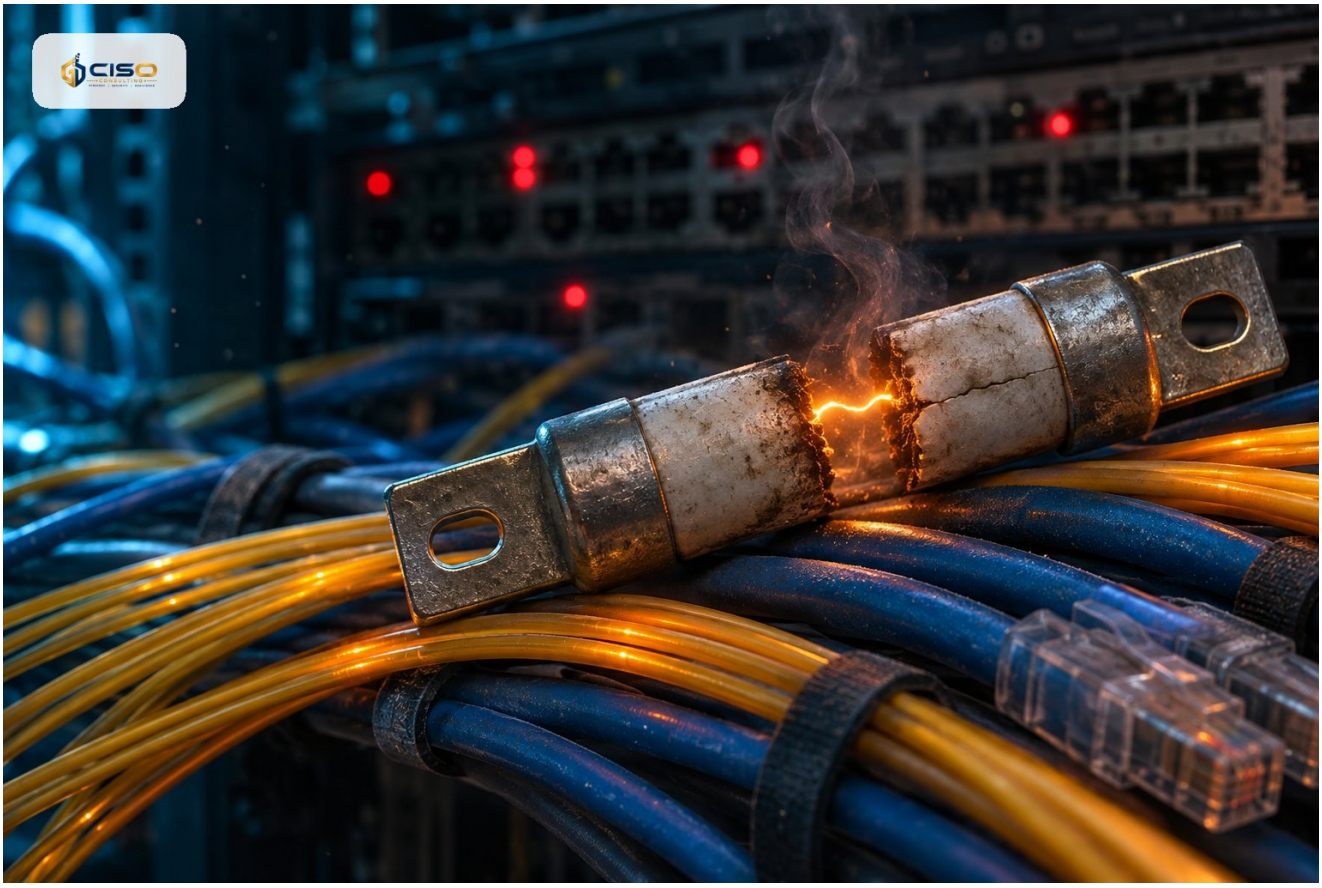
Siemens SENTRON 3NA COM Fuse: denial-of-service flaw (CVE-2024-7322) affects versions before 5.2



CISA has published an advisory on a denial-of-service vulnerability, CVE-2024-7322, in Siemens SENTRON 3NA COM Fuse versions below 5.2. Recovery may require the affected network to be re-established.

- Affected: SENTRON 3NA COM Fuse versions earlier than V5.2.
- CVE-2024-7322 is a denial-of-service issue linked to improper verification of the source of a communication channel.
- A ZigBee device may change its node ID on receiving an unsolicited encrypted rejoin response, causing the DoS.
- Recovery may require the network to be re-established.
- The vendor-assigned CVSS v3 score is 5.8.

CISA has released an advisory covering a denial-of-service vulnerability in the Siemens SENTRON 3NA COM Fuse. The flaw is tracked as CVE-2024-7322 and affects all versions earlier than V5.2. The vendor-assigned CVSS v3 score is 5.8.

What the issue is

The weakness is described as improper verification of the source of a communication channel. A ZigBee coordinator, router or end device may change its node ID when it receives an unsolicited encrypted rejoin response. That change causes a denial-of-service condition.

Successful exploitation may mean the affected network has to be re-established before normal operation returns.

Why it matters

CISA lists the product as deployed worldwide, with the vendor headquartered in Germany. The advisory names several critical infrastructure sectors, including critical manufacturing, energy, healthcare, financial services, transportation and government facilities. Organisations in the Kingdom that run electrical distribution monitoring in such environments should check whether this component is present.

The source excerpt does not detail remediation steps, so the Siemens and CISA advisories should be consulted directly for the fixed version and any mitigations.

Recommended approach

The rating is moderate, so a calm, planned response is appropriate: confirm exposure, review the vendor guidance and schedule the update through normal change control.

What to do now

1. Inventory OT and building-power environments for SENTRON 3NA COM Fuse and record the installed version.
2. Identify any units running a version earlier than V5.2.
3. Review the Siemens and CISA advisories for the fixed version and mitigations.
4. Schedule the update through change control, planning for possible network re-establishment.
5. Prepare a recovery procedure for restoring the ZigBee network if a DoS occurs.