CISA Flags Critical Vulnerabilities in EPICS Base 7.0.10 and Earlier



CISA has published an ICS advisory on EPICS Base 7.0.10 and earlier. The flaws carry a CVSS v3 score of 9.8 and could allow denial of service, memory corruption, data disclosure or code execution.

- Affected: EPICS Base release 7.0.10 and prior.
- Four CVEs are listed: CVE-2026-114595, CVE-2026-114596, CVE-2026-114597 and CVE-2026-114598.
- CVSS v3 score is 9.8; weakness types include integer overflow, length handling inconsistency and type confusion.
- Possible impact: denial of service, memory corruption, information disclosure, potentially arbitrary code execution.

> - The advisory lists the Critical Manufacturing sector, with worldwide deployment.

CISA has released an industrial control systems advisory covering EPICS Base, a product from The EPICS Community. Versions 7.0.10 and earlier are listed as known to be affected.

What the advisory says

Four vulnerabilities are listed: CVE-2026-114595, CVE-2026-114596, CVE-2026-114597 and CVE-2026-114598. They fall into three weakness types: **integer overflow or wraparound**, improper handling of length parameter inconsistency, and **type confusion**. The combined CVSS v3 score is 9.8.

For CVE-2026-114595, the advisory explains that an integer overflow in network request processing can cause memory to be allocated with the wrong size. Later handling of attacker-supplied data may then lead to memory corruption, denial of service, or potentially remote code execution.

Overall, successful exploitation could allow an attacker to cause denial of service, corrupt memory, disclose sensitive information, or possibly run arbitrary code. CISA lists the Critical Manufacturing sector and notes worldwide deployment.

What to do next

The excerpt we reviewed does not detail the vendor remediation steps, so teams should consult the full CISA advisory and the vendor's guidance. Institutions that run EPICS Base in industrial or research environments should first establish whether any instance is at version 7.0.10 or earlier, then plan mitigation according to the published remediation information.

What to do now

1. Inventory all EPICS Base deployments and identify any at version 7.0.10 or earlier.
2. Read the full CISA advisory and vendor guidance for the remediation and mitigation steps.
3. Plan and test updates or mitigations through change management before deploying to production.
4. Limit network exposure of affected systems and restrict access to them to required hosts only.
5. Monitor affected systems for crashes or unusual network requests and record findings in incident processes.