CISA flags critical flaws in Grid Protection Alliance openPDC and openHistorian



CISA published an ICS advisory on openPDC and openHistorian covering several vulnerabilities, with a CVSS v3 score of 9.8. Operators in the energy sector should identify affected versions and update.

- Affected: openPDC before 2.9.477 and 2.9.482, its Docker image, and openHistorian before 2.8.580 and 2.8.585.
- The advisory lists a CVSS v3 score of 9.8.
- Weakness types include unsafe deserialization, missing authentication for a critical function, SSRF, hard-coded credentials and unsafe reflection.
- CVE-2026-100730 concerns a service console that deserializes client-supplied data; on Windows Authentication systems the attacker must first be authenticated.

> - The advisory places the products in the energy sector, deployed worldwide.

CISA has published an industrial control systems advisory on openPDC and openHistorian, software from Grid Protection Alliance used in the energy sector. The advisory lists a CVSS v3 score of 9.8.

What is affected

The advisory names openPDC versions below 2.9.477 and 2.9.482, the openPDC Docker image in the same ranges, and openHistorian versions below 2.8.580 and 2.8.585. The listed CVEs are CVE-2026-104629, CVE-2026-100730, CVE-2026-105281, CVE-2026-85479 and CVE-2026-101022, with CVE-2026-105278 additionally listed for the Docker image.

The weakness types are deserialization of untrusted data, missing authentication for a critical function, server-side request forgery, use of hard-coded credentials, and unsafe reflection.

One example is CVE-2026-100730: a service console interface deserializes a data structure supplied by the client. Where Windows Authentication is used, an attacker must already be authenticated to reach the function. The excerpt we reviewed is truncated, so the full CISA advisory should be read for the remaining details.

What to do

Organizations running these products, particularly in energy and other operational technology environments, should confirm whether they use them and in which versions. Compare installed versions with the fixed ranges in the advisory and plan updates through normal change control. Until then, limit network access to the service console to those who need it.

What to do now

1. Check asset inventories for openPDC, its Docker image and openHistorian, and record the versions in use.
2. Compare versions against the fixed ranges in the CISA advisory and schedule updates through change management.
3. Restrict network access to the service console to authorized administrators and segment it from untrusted networks.
4. Review the full advisory, including each CVE description, for mitigations beyond updating.
5. Review logs on affected systems for unexpected access to the service console.