CISA flags two vulnerabilities in Subnet Solutions PowerSYSTEM Center



CISA published an advisory on two flaws in PowerSYSTEM Center, used in energy and critical manufacturing. They allow SQL command execution and access to restricted resources across the 2020, 2024 and 2026 versions.

- CVE-2026-63017 is an incorrect authorization flaw letting a low-privileged authenticated user reach administrator-only resources.
- CVE-2026-63774 is listed with SQL injection as the second weakness type; it affects the 2024 and 2026 lines.
- Affected: 2020 up to 5.29.x, 2024 from 6.0.x to 6.2.x, 2026 from 7.0.x to 7.1.x.
- The advisory shows a CVSS v3 score of 9 and names the energy and critical manufacturing sectors.
- The vendor is headquartered in Canada; the product is deployed worldwide.

CISA has released an industrial control systems advisory covering Subnet Solutions PowerSYSTEM Center. The advisory describes two vulnerabilities which, if exploited, could let an attacker run unauthorized SQL commands and reach resources they should not have access to.

What is affected

Three product lines are listed: PowerSYSTEM Center 2020 up to 5.29.x, PowerSYSTEM Center 2024 from 6.0.x to 6.2.x, and PowerSYSTEM Center 2026 from 7.0.x to 7.1.x. CVE-2026-63017 applies to all three; CVE-2026-63774 applies to the 2024 and 2026 lines.

CVE-2026-63017 is an incorrect authorization issue: a low-privileged, authenticated user can access resources normally limited to administrators. The advisory also lists improper neutralization of special elements in an SQL command (SQL injection) among the weaknesses. It shows a CVSS v3 score of 9 and lists Critical Manufacturing and Energy as the affected sectors.

What to do next

The source excerpt refers to vendor mitigation guidance for PowerSYSTEM Center 2024 users but does not give its full text. Operators should read the complete CISA advisory and the vendor's instructions before planning changes.

Organizations in energy and industrial operations should first establish whether PowerSYSTEM Center is present in their environment, which version runs, and who holds accounts on it. Because one flaw depends on an authenticated account, reviewing account privileges is a sensible early step while remediation is scheduled.

What to do now

1. Inventory any PowerSYSTEM Center 2020, 2024 or 2026 installations and record exact versions.
2. Read the full CISA advisory and the vendor's mitigation guidance, and plan remediation accordingly.
3. Review accounts on the platform and remove unneeded or excess low-privilege access.
4. Confirm the platform is not reachable from untrusted networks and that access is restricted to required users.
5. Monitor database and application logs for unusual queries or administrator-level activity by ordinary accounts.