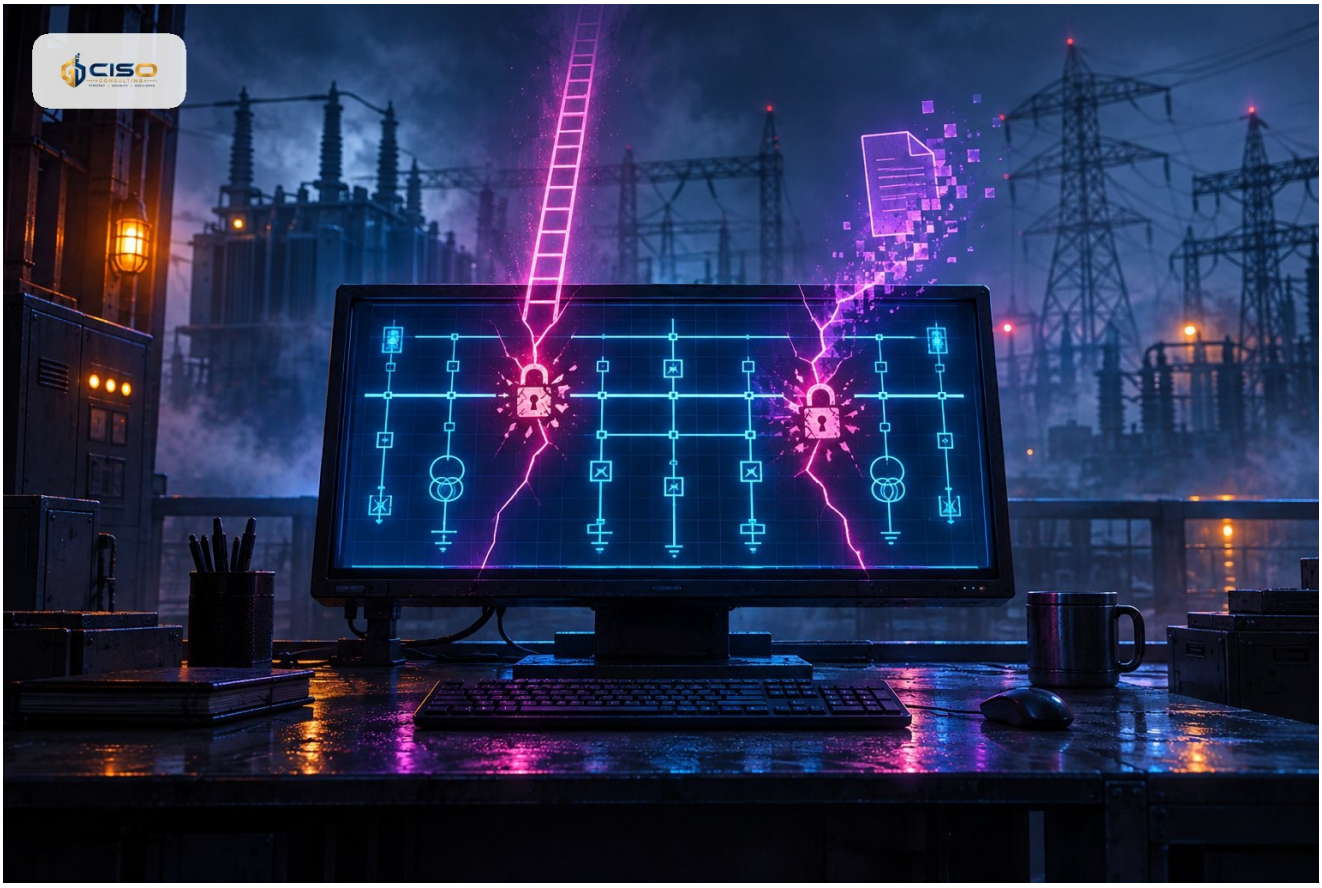
CISA flags two vulnerabilities in ABB PCM600 up to version 2.14



CISA published an advisory on ABB PCM600 up to version 2.14. Two flaws, CVE-2026-15952 and CVE-2026-15953, could allow privilege escalation or file overwrite. CVSS v3 score is 6.4.

- Affected: ABB Protection and Control IED Manager PCM600, versions up to and including 2.14.
- CVE-2026-15952 concerns the Scheduler Service, which runs as LocalSystem while standard PCM600 users hold permissions over it.
- Exploitation needs local access and valid user credentials, and could give control of the host.
- The second flaw, CVE-2026-15953, is a path traversal weakness; the advisory lists file overwrite as a possible impact.
- The advisory lists the Energy sector, worldwide deployment, and a CVSS v3 score of 6.4.

What was published

CISA issued an ICS advisory covering ABB Protection and Control IED Manager PCM600, versions up to and including 2.14. Two vulnerabilities are listed: CVE-2026-15952 and CVE-2026-15953. The advisory states that successful exploitation could let an attacker escalate privileges or overwrite files. The CVSS v3 score is 6.4. ABB is headquartered in Switzerland, and the advisory tags the product to the Energy sector with worldwide deployment.

Technical detail

CVE-2026-15952 involves the Scheduler Service installed with PCM600. The service runs under the LocalSystem account, yet permissions on it are granted to standard PCM600 users through membership in the local users group. An attacker with local access and valid user credentials could use this to elevate privileges and take control of the affected host. The second issue, CVE-2026-15953, is classed as a path traversal weakness (improper limitation of a pathname to a restricted directory). The excerpt provided does not describe it in further detail.

Practical reading

Both issues depend on an attacker already having a foothold on the machine, so the exposure is mainly about who can log on to engineering workstations that run PCM600. Institutions in the energy and utilities space should confirm whether PCM600 is in use and which version is installed. The source excerpt does not state whether a fixed version is available, so check the full CISA advisory and ABB's own notice for remediation guidance.

What to do now

1. Inventory all hosts running PCM600 and record the installed version against the 2.14 threshold.
2. Review the full CISA advisory and ABB's notice for fixes or mitigations and plan their deployment.
3. Restrict interactive and remote logon to PCM600 workstations to named, necessary engineers.
4. Review membership of the local users group on those hosts and remove accounts that do not need access.
5. Monitor these workstations for unexpected privilege changes or file modifications, in line with OT security controls.