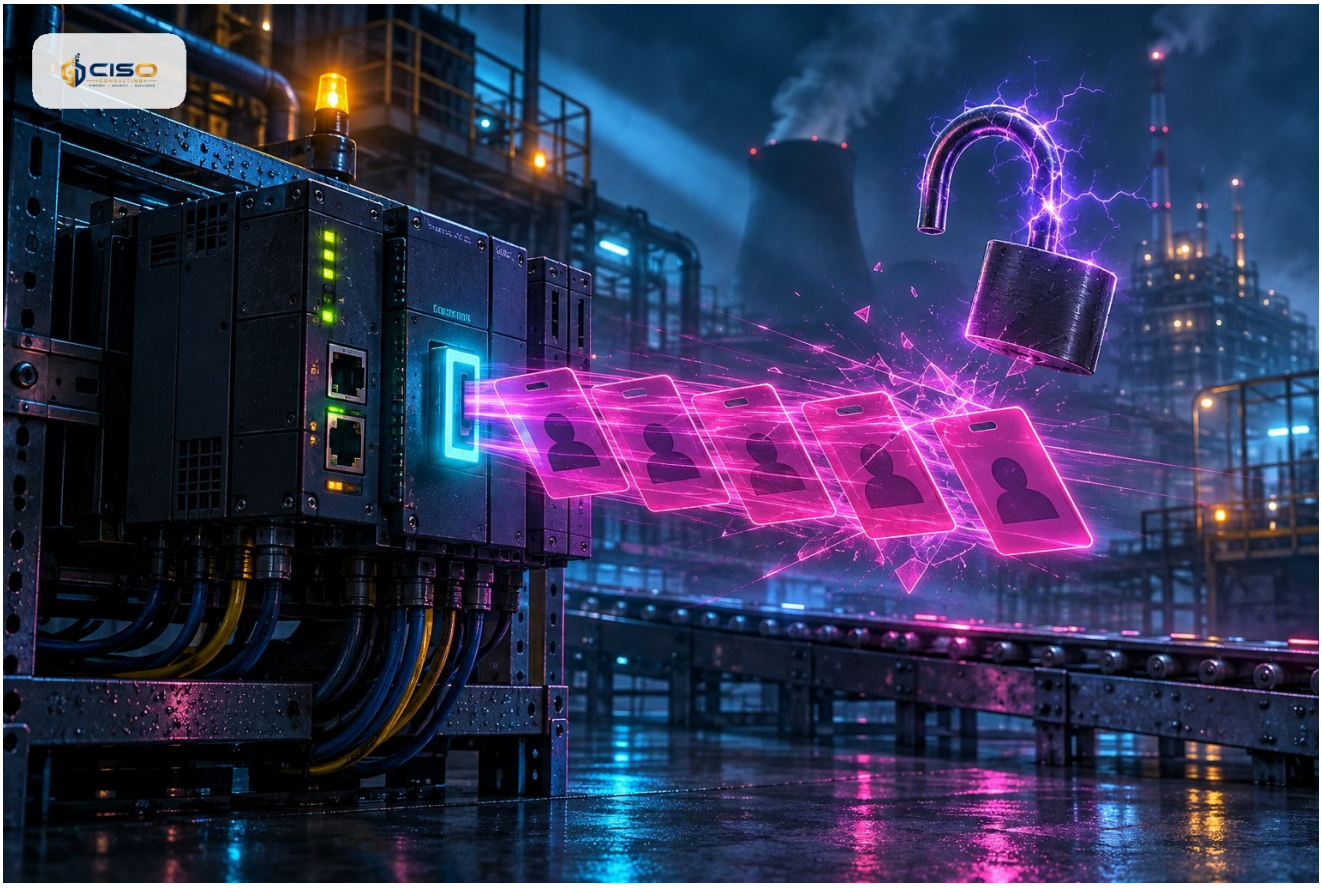
CISA flags race condition in OpenPLC Runtime that allows unauthenticated admin account creation



CISA reports CVE-2026-126088 in Autonomy Logic OpenPLC Runtime 4.2.4 and earlier, where a race condition can create several unauthenticated admin accounts. The vendor fix is version 4.3.0 or later.

- Affected: Autonomy Logic OpenPLC Runtime version 4.2.4 and prior.
- CVE-2026-126088 is a race condition (CWE-362) with a CVSS v3 score of 8.1.
- Concurrent requests pass the existence check before any user is committed, so several unauthenticated admin accounts can be created.
- The vendor fix is to update to OpenPLC Runtime 4.3.0 or later.
- Listed sectors: critical manufacturing, energy, transportation systems, and water and wastewater.

CISA has published an industrial control systems advisory on Autonomy Logic OpenPLC Runtime, covering a single vulnerability tracked as CVE-2026-126088. It affects versions 4.2.4 and earlier.

What the issue is

The flaw is a race condition (CWE-362). When several requests arrive at the same time, they can all pass the check for whether a user already exists before any account has been saved. The result, according to the advisory, is that several unauthenticated admin accounts can be created. The issue carries a CVSS v3 score of 8.1.

The advisory lists critical manufacturing, energy, transportation systems, and water and wastewater systems as relevant sectors, with worldwide deployment. The vendor is headquartered in the United States.

What to do

The vendor's remediation is to update to OpenPLC Runtime 4.3.0 or later. Organisations that run OpenPLC Runtime in operational technology environments should first establish whether any instance is on 4.2.4 or earlier, then plan the update through their normal OT change process. The source does not describe exploitation in the wild or other workarounds, so we do not speculate on them.

Because the outcome is unauthorised administrative access, it is also sensible to review existing accounts on affected instances for any that are unexpected.

What to do now

1. Inventory all OpenPLC Runtime instances and identify any on version 4.2.4 or earlier.
2. Update affected instances to OpenPLC Runtime 4.3.0 or later through the OT change-management process.
3. Review user accounts on affected instances and investigate any unexpected admin accounts.
4. Confirm that OpenPLC management interfaces are not reachable from untrusted networks.
5. Record the vulnerability and remediation status in the OT risk register.