Hitachi Energy REB500 up to 8.3.3.1: open-source flaws can cause denial of service



CISA reports two open-source library vulnerabilities (CVE-2024-8176, CVE-2025-59375) in Hitachi Energy REB500 versions up to 8.3.3.1 that can enable denial of service. Review the vendor's recommended actions.

- Affected: Hitachi Energy REB500 versions up to and including 8.3.3.1.
- Two CVEs: CVE-2024-8176 and CVE-2025-59375, both in open-source software components.
- Impact: denial of service; for CVE-2024-8176, memory corruption is possible in some environments.
- CVE-2024-8176 is a stack overflow in libexpat, used by the IEC 61850 functionality, triggered by a crafted message from an authenticated user with local access.
- Vendor CVSS v3 score is 6.5; the product is deployed in the energy sector worldwide.

CISA has published an advisory on Hitachi Energy's REB500 product, covering vulnerabilities in open-source software it contains. Hitachi Energy states that these flaws can be used to mount a denial-of-service attack against the product.

What is affected

All REB500 versions up to and including 8.3.3.1 are listed as affected. The advisory names two CVEs, CVE-2024-8176 and CVE-2025-59375, and the vendor rates the issues at CVSS v3 6.5. The weakness types are uncontrolled recursion and allocation of resources without limits or throttling.

CVE-2024-8176 is a stack overflow in the libexpat library, which the IEC 61850 functionality of REB500 relies on. An authenticated user with local access could send a crafted IEC 61850 message to trigger it. Depending on the environment and how the library is used, the result may be denial of service or, in some cases, exploitable memory corruption.

How to read this

The described attack path requires authentication and local access, which limits exposure but does not remove it where accounts or local access are loosely controlled. The advisory lists the energy sector as the affected critical infrastructure and notes worldwide deployment.

Next steps

The advisory points to the vendor's Recommended Immediate Actions for mitigation and remediation. Operators should identify any REB500 units, confirm their version, and follow that guidance through their normal change process for operational technology.

What to do now

1. Inventory all REB500 units and confirm whether any run version 8.3.3.1 or earlier.
2. Read Hitachi Energy's Recommended Immediate Actions and plan mitigation or remediation for affected units.
3. Restrict local access and review authenticated accounts on REB500 devices, since exploitation needs both.
4. Restrict and monitor IEC 61850 traffic reaching affected devices.
5. Record the exposure and remediation status in your OT risk register under NCA OTCC requirements.