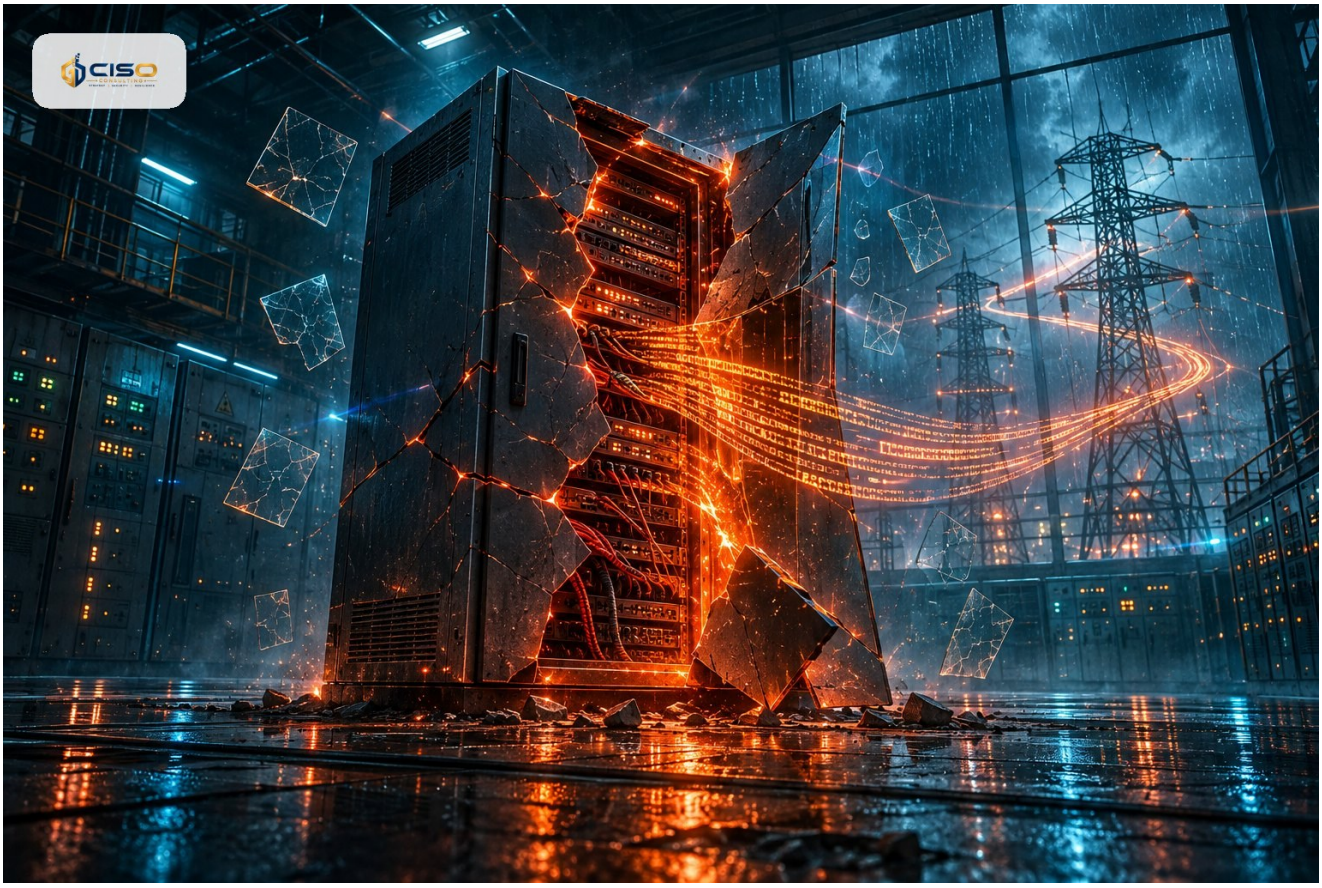
Hitachi Energy CoreTec: OS Command Injection and Dirty Frag Flaws Reported



CISA has published an advisory on two vulnerabilities in Hitachi Energy CoreTec 4 and 5, an OS command injection and a Dirty Frag flaw. Exploitation could affect confidentiality, integrity and availability of the product.

- Affected: CoreTec5 up to 3.4.0 and 5.0.0 (CVE-2026-13162, CVE-2026-43284); CoreTec4 up to 3.4.0 (CVE-2026-13162).
- CVE-2026-13162 lets authenticated users with certain roles run arbitrary system commands with full control of the device.
- The vendor CVSS v3 score is 8.8.
- The second flaw is a write-what-where condition (Dirty Frag).
- The advisory lists the Energy sector, with worldwide deployment.

What was reported

CISA has republished a Hitachi Energy advisory covering the CoreTec product line. Two vulnerabilities are described: an OS command injection (CVE-2026-13162) and a write-what-where condition known as Dirty Frag (CVE-2026-43284).

CVE-2026-13162 affects both CoreTec4 and CoreTec5. It allows an authenticated user holding certain roles to run arbitrary system commands, giving full control over the device. CVE-2026-43284 is listed for CoreTec5 only.

Affected versions

- CoreTec5: versions up to 3.4.0, and 5.0.0
- CoreTec4: versions up to 3.4.0

The vendor rates the issue at CVSS v3 8.8. Successful exploitation could affect the confidentiality, integrity and availability of the product. The advisory places the product in the Energy sector.

Why it matters

Because exploitation requires an authenticated account with specific roles, control of privileged access and of the network paths to these devices is central to reducing exposure. Operators should consult the vendor's recommended immediate actions for the exact mitigation and remediation steps.

What to do now

1. Identify any CoreTec4 or CoreTec5 devices in your OT estate and check their versions against the affected list.
2. Apply the mitigation and remediation steps in the vendor's recommended immediate actions.
3. Review which accounts hold elevated roles on these devices and remove those not needed.
4. Restrict network access to device management interfaces to approved segments only.
5. Record the exposure in the OT risk register in line with NCA OTCC requirements.