

Hitachi Energy RTU500 CMU Firmware: CISA Lists Multiple Vulnerabilities



CISA has published an advisory on vulnerabilities in the CMU firmware of Hitachi Energy RTU500 series products. Exploitation could affect confidentiality, integrity and availability. Operators should review the affected versions.

- The advisory covers the CMU firmware of the Hitachi Energy RTU500 series.
- Affected ranges: 12.7.1–12.7.7, 13.5.1–13.5.4, 13.6.1–13.6.3, 13.7.1–13.7.8 and 13.8.1–13.8.2.
- Listed CVEs include CVE-2026-17539, CVE-2026-28388, CVE-2026-6732, CVE-2026-6653 and CVE-2026-6276, among others.
- Exploitation could affect confidentiality, integrity and availability of the product.
- The vendor points to Recommended Immediate Actions for mitigation and remediation.

What was published

CISA has released an industrial control systems advisory on Hitachi Energy RTU500 series products. Hitachi Energy states that it is aware of vulnerabilities in the CMU firmware which, if exploited, could affect the confidentiality, integrity and availability of the product.

The affected CMU firmware ranges are 12.7.1 to 12.7.7, 13.5.1 to 13.5.4, 13.6.1 to 13.6.3, 13.7.1 to 13.7.8 and 13.8.1 to 13.8.2. The advisory lists several CVEs, including CVE-2026-17539, CVE-2026-28388, CVE-2026-6732, CVE-2026-6653, CVE-2026-6276, CVE-2026-9079, CVE-2026-11856, CVE-2026-8927 and CVE-2026-8932.

What the source does not say

The excerpt available to us does not give severity scores, technical details of each flaw, or any report of exploitation in the wild. We therefore make no claim on those points. The full advisory and the vendor's Recommended Immediate Actions should be treated as the authoritative reference.

Suggested approach

Organisations operating RTU500 equipment, such as utilities and other critical infrastructure operators, should first confirm whether their CMU firmware falls inside the listed ranges, then follow the vendor's mitigation and remediation guidance through their normal OT change process.

What to do now

1. Identify all RTU500 units and record their CMU firmware versions against the affected ranges.
2. Read the full CISA advisory and Hitachi Energy's Recommended Immediate Actions, then plan mitigation or remediation.
3. Schedule remediation through the OT change-management process, with testing and a rollback plan.
4. Review network exposure of RTU500 devices and confirm they sit in segmented OT zones.
5. Report affected assets and the remediation status to the OT risk owner under NCA OTCC requirements.