# Hitachi Energy TRO600 series: two vulnerabilities allow remote code execution and data disclosure



CISA published an advisory on two vulnerabilities in Hitachi Energy TRO600 series products. They could allow remote code execution and disclosure of sensitive information. The vendor lists CVSS v3 7.5.

- Two vulnerabilities, CVE-2026-10756 and CVE-2026-106087, affect the TRO600 series.
- Affected versions include TRO600 up to 9.2.1.6 and up to 9.1.1.0, plus 9.2.2.1 and 9.1.2.0.
- The weaknesses are improper restriction of communication channels and missing authentication for a critical function.
- CVE-2026-10756 lets an authenticated attacker bypass network restrictions and reach services meant only for localhost, using port forwarding.
- The vendor rates the issue CVSS v3 7.5; the affected sector is energy, with worldwide deployment.

CISA has published an industrial control systems advisory covering Hitachi Energy TRO600 series products. According to the advisory, the vulnerabilities can be exploited for remote code execution to support further attacks, and for disclosure of sensitive information.

## What is affected

Two vulnerabilities are listed: CVE-2026-10756 and CVE-2026-106087. The affected versions are TRO600 up to 9.2.1.6, TRO600 up to 9.1.1.0, and versions 9.2.2.1 and 9.1.2.0. The vendor assigns a CVSS v3 score of 7.5. The weakness classes are improper restriction of communication channel to intended endpoints and missing authentication for a critical function.

For CVE-2026-10756, an authenticated attacker can bypass network access restrictions and reach services intended to be available only from localhost. By using port forwarding, the attacker can interact with locally bound ports and services.

## Context

The advisory places the products in the energy sector, deployed worldwide, with the vendor headquartered in Switzerland. The published excerpt does not describe exploitation in the wild, so organisations should treat this as a patching and exposure-review task rather than an emergency.

## Recommended approach

Hitachi Energy directs users to the Recommended Immediate Actions section of the advisory for mitigation and remediation. Operators should confirm whether TRO600 devices are in their estate, identify firmware versions and follow the vendor's guidance.

## What to do now

1. Inventory TRO600 devices across operational and remote sites and record their firmware versions.
2. Compare versions against the affected list and follow the vendor's Recommended Immediate Actions.
3. Restrict access to device management interfaces and limit accounts able to authenticate to them.
4. Review logs for unexpected port forwarding or connections to local-only services on these devices.
5. Record the finding in the OT risk register and report per NCA OTCC and internal procedures where applicable.