

Hitachi Energy MicroSCADA X SYS600: CSV injection and authentication flaws disclosed



CISA published an advisory on vulnerabilities in Hitachi Energy MicroSCADA X SYS600 versions up to 10.7 and 10.8, including CSV formula injection and a flawed authentication algorithm. The vendor CVSS v3 score is 7.8.

- Affected: MicroSCADA X SYS600 versions up to 10.7, and 10.8.
- Listed CVEs: CVE-2026-9852, CVE-2026-9853 and CVE-2026-9854.
- Weakness types: improper neutralization of formula elements in CSV files, and incorrect implementation of an authentication algorithm.
- Vendor CVSS v3 score is 7.8; the product is used in the energy sector.
- Hitachi Energy provides mitigation and remediation steps under Recommended Immediate Actions.

What was disclosed

CISA has published an industrial control systems advisory covering multiple vulnerabilities in Hitachi Energy MicroSCADA X SYS600. The affected versions are those up to and including 10.7, as well as 10.8. The advisory lists CVE-2026-9852, CVE-2026-9853 and CVE-2026-9854, and the vendor-assigned CVSS v3 score is 7.8.

Two weakness categories are named: improper neutralization of formula elements in a CSV file, and incorrect implementation of an authentication algorithm. The product is associated with the energy sector, is deployed worldwide, and the vendor is headquartered in Switzerland.

The CSV injection issue

For CVE-2026-9852, the advisory describes a CSV injection flaw in SYS600. Malicious formulas placed in exported data can add or change spreadsheet content, insert links, or exfiltrate data. Depending on how the user's environment is configured, they may also run malicious code on the user's machine. The excerpt provided does not give the full exploitation conditions or details of the other CVEs.

What to do next

The vendor directs customers to its Recommended Immediate Actions for mitigation and remediation. Operators of SYS600 should confirm whether they run an affected version, review the full advisory and vendor guidance, and plan remediation through their normal change process for operational technology.

What to do now

1. Identify all SYS600 instances and check whether they run version 10.7 or earlier, or 10.8.
2. Read the full CISA advisory and Hitachi Energy's Recommended Immediate Actions, then schedule mitigation or remediation.
3. Until remediation, treat CSV files exported from SYS600 as untrusted and avoid opening them with spreadsheet macros or formula features enabled.
4. Review access to SYS600 and its network segmentation as part of OT risk management.
5. Record the exposure and remediation plan in the OT risk register.