

Hitachi Energy Asset Suite Vulnerable to Unauthenticated Servlet Access



CISA reports critical authentication bypass vulnerabilities in Hitachi Energy Asset Suite versions 9.9.0 and earlier, enabling unauthenticated access to test servlets that may compromise confidentiality and integrity.

- Two vulnerabilities (CVE-2026-7395, CVE-2026-11796) affect Asset Suite versions 9.9.0 and earlier
- Unauthenticated users can access HTTPPublishAdapterTestServlet intended for testing environments only
- Exploitation may lead to configuration file upload, information disclosure and integrity compromise
- CVSS v3 score of 8.1 indicates high severity with potential confidentiality, integrity and availability impact
- Vulnerabilities affect energy sector infrastructure deployed worldwide

Vulnerability Overview

The United States Cybersecurity and Infrastructure Security Agency has published an advisory concerning authentication bypass vulnerabilities in Hitachi Energy Asset Suite. The flaws affect all versions up to and including 9.9.0 and are tracked as CVE-2026-7395 and CVE-2026-11796. With a CVSS v3 base score of 8.1, these vulnerabilities represent a **missing authentication for critical function** weakness that may be exploited by unauthenticated actors.

The primary vulnerability permits unauthorized access to HTTPPublishAdapterTestServlet, a component designed exclusively for testing in non-production environments. Successful exploitation enables attackers to upload configuration files, potentially leading to information disclosure and integrity compromise. The vulnerabilities pose risks to confidentiality, integrity and availability of affected systems.

Energy Sector Implications

Asset Suite is deployed globally within the energy sector, classified as critical infrastructure. Organizations operating energy facilities, substations or related operational technology environments using this platform should treat this advisory as requiring immediate attention. The Switzerland-based vendor has acknowledged the vulnerabilities and provided mitigation guidance.

Mitigation Guidance

Hitachi Energy has issued recommended immediate actions for affected deployments. Institutions should consult the vendor's official remediation documentation and evaluate whether test servlets are exposed in production environments. Network segmentation and access controls should be reviewed to ensure testing components are isolated from operational networks.

What to do now

1. Inventory all deployments of Hitachi Energy Asset Suite within your operational technology environment and confirm version numbers
2. Review network architecture to verify that HTTPPublishAdapterTestServlet and similar testing components are not accessible from production networks
3. Consult Hitachi Energy's official remediation guidance and apply vendor-recommended mitigations immediately for affected versions
4. Implement network segmentation to isolate testing and development environments from operational control systems
5. Monitor access logs for unusual activity targeting servlet endpoints, particularly unauthenticated access attempts
6. Coordinate with your OT security team to schedule patching or compensating controls in accordance with NCA OTCC change management requirements