



An Láirionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2610130333

NCSC Advisory

Critical Vulnerability in Ivanti Connect Secure

CVE-2026-104935

13th, October 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>. Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-104935**Published:** 2026-10-13**Vendor:** Ivanti**Product:** Connect Secure**CVSS Score¹:** 8.6

Products Affected

Product	Version	Resolved Version
Ivanti Connect Secure (ICS)	25.1.1.1 and prior	25.1.1.2
	25.1.2.2 and prior	25.1.3.0, 25.1.3.1
	22.8R2.4 and prior	22.8R2.5

Impact

Authentication bypass by spoofing in ICS before version 25.1.3.0 allows a remote unauthenticated attacker to execute arbitrary commands. This does not impact ICS version 22.7R2.14 or prior.

Common Weakness Enumeration (CWE)²: CWE-290 Authentication bypass by spoofing

Known Exploited Vulnerability (KEV) catalog³: Yes

Used by Ransomware Operators: N/A

¹ <https://www.first.org/cvss/>

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Ivanti.

- <https://nvd.nist.gov/vuln/detail/CVE-2026-104935>
- <https://www.cve.org/CVERecord?id=CVE-2026-104935>
- <https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935>
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-104935

