

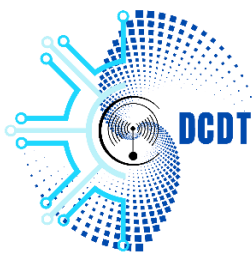
**GOVERNMENT OF THE REPUBLIC  
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU  
DEPARTMENT OF COMMUNICATIONS  
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA  
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE  
COMMUNICATION ET DE  
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

14 October 2026

**Advisory 354: Ivanti Connect Secure Authentication Bypass Remote Command Execution Vulnerability - Actively Exploited Zero-Day (CVE-2026-104935).**

**Release Date:** 13<sup>th</sup> October 2026

**Impact:** **CRITICAL**

**TLP:** CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

## What is it?

CVE-2026-104935 is an authentication bypass by spoofing vulnerability (CWE-290) in Ivanti Connect Secure (ICS), the SSL VPN gateway. A remote attacker with no credentials and no user interaction can bypass authentication and run arbitrary commands on the appliance. Ivanti has confirmed limited exploitation in the wild. It is scored CVSS 8.6 (High) by third-party sources, and CERTVU rates it CRITICAL because it is unauthenticated, sits on an internet-facing VPN gateway and is a zero-day under active exploitation.

## What are the systems affected?

The following Ivanti Connect Secure releases are affected:

- ICS 22.8R2.4 and earlier
- ICS 25.1.1.1 and earlier, and 25.1.2.2 and earlier
- Only Connect Secure is named in the advisory; Policy Secure, ZTA Gateways and Neurons for Secure Access are not listed as affected

The privilege escalation flaw in the same attack chain remained unpatched at the time of writing, so check Ivanti for a further update.

Not affected / patched version:

- ICS 22.8R2.5 (Ivanti advises 22.8 customers to move to 25.1.1.2), 25.1.1.2, 25.1.3.0 or 25.1.3.1, depending on your release train

## What does this mean?

Successful exploitation may allow attackers to:

- Bypass VPN gateway authentication and run commands on the appliance without any credentials
- Steal domain credentials and Active Directory data stored on or reachable from the appliance, including LAPS passwords and BitLocker recovery keys
- Use the gateway as a foothold for password spraying, network scanning and lateral movement into the internal network, while altering logs to hide the activity

## Mitigation process

CERTVU recommends the following:

### 1. Upgrade now

Upgrade every ICS appliance to the fixed release for your branch listed above. Ivanti describes no workaround, so patching is the only fix. Upgrading closes the entry point but does not remove an attacker who is already in.

### 2. Inventory all appliances

Identify every ICS appliance, including internal and test units, and record the exact build number.

### 3. Hunt for compromise

### 4. Rotate credentials

## Reference

1. <https://www.securityweek.com/ivanti-zero-day-chain-gave-attackers-root-access-to-fully-patched-vpn/>
2. <https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-day-exploited-in-attacks/>
3. <https://www.cisa.gov/news-events/alerts/2026/10/13/cisa-adds-two-known-exploited-vulnerabilities-catalog>
4. <https://nvd.nist.gov/vuln/detail/CVE-2026-104935>