Vulnerability Advisory

TLP: CLEAR

CAL-CSIC-2026-10-A-013

13 OCT 2026

Authentication Bypass Vulnerability Actively Exploited within Ivanti Connect Secure

Authentication Bypass	Code Execution	Active Exploitation Confirmed	Fixed Releases Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high-severity vulnerability affecting Ivanti Connect Secure (ICS) VPN appliances. The vulnerability, CVE-2026-104935, carries a CVSS 3.1 score of 8.6. Ivanti Connect Secure provides secure remote access to corporate applications and resources from any device using zero-trust controls.[1]

CVE-2026-104935 involves spoofed request routing that exposes protected functionality and enables code execution. Exploitation was observed beginning on 03 October 2026 against an ICS appliance. The attacker chained this vulnerability with a separate privilege escalation flaw to obtain root access, steal credentials, collect directory data, and prepare for lateral movement. Open-source reporting states that a fix for the separate privilege escalation flaw is ongoing and will be included in a future release in the coming weeks.[2]

Ivanti has acknowledged limited exploitation in the wild and released updates for affected versions. ICS 22.7R2.14 and earlier are not affected. Administrators should use the fixed release appropriate to their appliance and release branch.[3]

The Cal-CSIC recommends applying Ivanti's updates immediately upon availability, reviewing available indicators of compromise, and following Ivanti's recovery guidance if exploitation is suspected. Run the Integrity Checker Tool regularly; however, a clean result cannot rule out this attack chain.

For additional details regarding CVE-2026-104935, please use this link:

Ivanti Security Advisory:

https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935

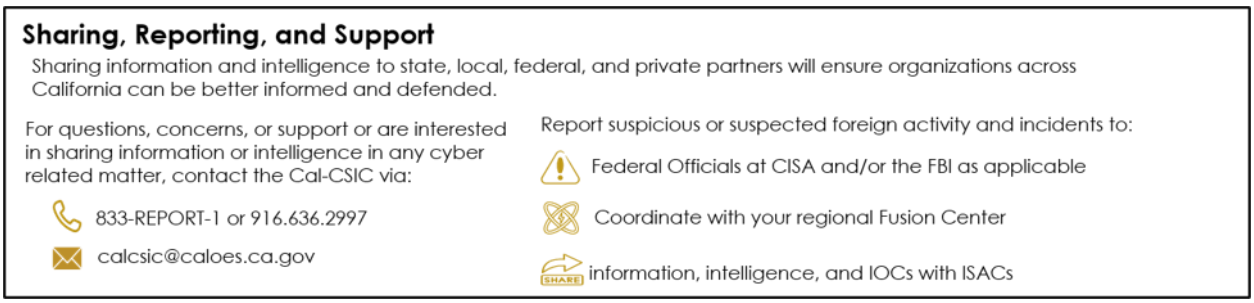
WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Affected Products and Versions

Product	Affected Version	Fixed Release
Ivanti Connect Secure	25.1.1.1 and earlier	25.1.1.2
Ivanti Connect Secure	25.1.2.2 and earlier	25.1.3.0 or 25.1.3.1
Ivanti Connect Secure	22.8R2.4 and earlier	22.8R2.5

Note: ICS 22.7R2.14 and earlier are not affected. For the 22.8 branch, Ivanti recommends migration to 25.1.1.2 or later; 22.8R2.5 is available for customers unable to migrate immediately.

Sharing, Reporting, and Support



References

[1] Ivanti; "Ivanti Connect Secure: Secure Access VPN for the Everywhere Workplace"; https://www.ivanti.com/resources/library/datasheets/ivi-2516-connect-secure-ds/?ext=pdf; accessed 13 October 2026

[2] Volexity; "A Series of Unauthenticated Events: Chained Exploitation of Ivanti Connect Zero-Days"; https://www.volexity.com/blog/2026/10/13/a-series-of-unauthenticated-events-chained-exploitation-of-ivanti-connect-secure-zero-days/; accessed 13 October 2026

[3] Ivanti Innovators Hub; "Security Advisory Ivanti Connect Secure (CVE-2026-104935)"; https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US; accessed 13 October 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.