CYBER ADVISORY

TLP:CLEAR

31 January 2024

Ivanti Connect Secure and Policy Secure Vulnerabilities

CVE-2024-21888 | CVE-2024-21893 | Connect Secure | Active Exploitation

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of two high vulnerabilities known as CVE-2024-21888 and CVE-2024-21893.[1] CVE-2024-21888 is a privilege escalation vulnerability in the web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x). Exploitation of the vulnerability could allow an attacker to elevate privileges to that of an administrator.[2] CVE-2024-21893, which is under active exploitation, is a server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA. Exploitation of the vulnerability could allow an attacker to access certain restricted resources without authentication.[3,4]

The Cal-CSIC recommends immediately applying the appropriated patches or mitigation efforts to the affected Ivanti software.

For further information on implementing mitigation, please refer to Ivanti Forums.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] The Hacker News; "Alert: Ivanti Discloses 2 New Zero-Day Flaws, One Under Active Exploitation;" https://thehackernews.com/2024/01/alert-ivanti-discloses-2-new-zero-day.html; accessed 31 January 2024

[2] Bleeping Computer; "Ivanti warns of new Connect Secure zero-day exploited in attacks;" https://www.bleepingcomputer.com/news/security/ivanti-warns-of-new-connect-secure-zero-day-exploited-in-attacks/; accessed 31 January 2024

[3] Ivanti; "Security Update for Ivanti Connect Secure and Ivanti Policy Secure Gateways;" https://www.ivanti.com/blog/security-update-for-ivanti-connect-secure-and-ivanti-policy-secure-gateways; accessed 31 January 2024

[4] Ivanti; "CVE-2024-21888 Privilege Escalation for Ivanti Connect Secure and Ivanti Policy Secure;" https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US; accessed 31 January 2024