CYBER ADVISORY

TLP:CLEAR
12 February 2024

Ivanti SAML Vulnerability

CVE-2024-22024 | Connect Secure | Policy Secure | High Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high vulnerability, known as CVE-2024-22024.[1] The Vulnerability affects Ivanti Connect Secure (version 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2, 22.5R1.1, and 22.5R2.2), Ivanti Policy Secure version 22.5R1.1 and ZTA version 22.6R1.3.[2] Vulnerability lies in the Security Assertion Markup Language, (SAML) component which may allow an attacker to access certain restricted resources without authentication.[3]

The Cal-CSIC recommends to immediately apply appropriated upgrades.

For further information on applying upgrades, please refer to Ivanti Upgrade Guide.

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] Tenable; "CVE-2024-22024;" https://www.tenable.com/cve/CVE-2024-22024; accessed 12 February 2024
[2] Ivanti; "CVE-2024-22024 (XXE) for Ivanti Connect Secure and Ivanti Policy Secure;" https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US; accessed 12 February 2024
[3] watchTowr Labs; "Ivanti Connect Secure CVE-2024-22024 - Are We Now Part Of Ivanti?;" https://labs.watchtowr.com/are-we-now-part-of-ivanti/; accessed 12 February 2024