CYBER ADVISORY

TLP:CLEAR

11 January 2024

Ivanti Zero-Day Vulnerabilities

CVE-2023-46805 | CVE-2024-21887 | Zero Day | Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of zero-day vulnerabilities under active exploitation known as CVE-2023-46805, CVE-2024-21887.[1] The vulnerabilities affect Ivanti Connect Secure and Ivanti Policy Secure Gateways.[2] Exploitation of CVE-2023-46805 could allow attackers to bypass authentication, including multi-factor authentication. CVE-2024-21887 is a command injection vulnerability in the devices' web component that could allow authenticated attackers to send specially crafted requests and execute arbitrary commands on the appliance. Used in conjunction, exploitation does not require authentication and could enable a threat actor to craft malicious requests and execute arbitrary commands on the system. [3,4]

The Cal-CSIC recommends immediately applying Ivanti recommended mitigations.

For further information on applying mitigations, 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 here.
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] Help Net Security; "Ivanti Connect Secure zero-days exploited by attackers (CVE-2023-46805, CVE-2024-21887);" https://www.helpnetsecurity.com/2024/01/11/cve-2023-46805-cve-2024-21887/; accessed 11 January 2024

[2] CISA; "Ivanti Releases Security Update for Connect Secure and Policy Secure Gateways;" https://www.cisa.gov/news-events/alerts/2024/01/10/ivanti-releases-security-update-connect-secure-and-policy-secure-gateways; accessed 11 January 2024

[3] Ivanti; "CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways;" https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US; accessed 11 January 2024

[4] Bleeping Computer; "Ivanti warns of Connect Secure zero-days exploited in attacks;" https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-days-exploited-in-attacks/; accessed 11 January 2024