Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

*CYBER ADVISORY*

TLP:CLEAR
11 July 2024

# Palo Alto Network Expedition: Missing Authentication Vulnerability

CVE-2024-5910 | Remote Code Execution | Missing Authentication | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability that is highly likely to be exploited known as CVE-2024-5910.[1] This affects Palo Alto Networks Expedition version 1.2.91 or below. This vulnerability stems from a missing authentication for a critical function in Palo Alto Networks Expedition which can lead to an Expedition admin account takeover for attackers with network access to Expedition.

The Cal-CSIC recommends immediately upgrading to latest version of Expedition 1.2.92.

## 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] Palo Alto Networks; "CVE-2024-5910 Expedition: Missing Authentication Leads to Admin Account Takeover" https://security.paloaltonetworks.com/CVE-2024-5910; 10 July 2024

**WARNING:** This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.