CYBER ADVISORY

TLP:CLEAR
25 November 2024

PAN-OS Management Web Interface Vulnerabilities

CVE-2024-0012 | CVE-2024-9474 | Exploited | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-0012 (CVSS 3.1: 9.3)[1] and a medium severity vulnerability known as CVE-2024-9474 (CVSS 3.1: 6.9).[2] The two vulnerabilities are actively exploited in a vulnerability chain, allowing an attacker to exploit the public-facing Management Web Interface in Palo Alto Network's PAN-OS operating system (CVE-2024-0012) resulting in the escalation of privileges to gain root level permissions (CVE-2024-9474).[3][4]

Version	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 11.2	< 11.2.4-h1	>= 11.2.4-h1
PAN-OS 11.1	< 11.1.5-h1	>= 11.1.5-h1
PAN-OS 11.0	< 11.0.6-h1	>= 11.0.6-h1
PAN-OS 10.2	< 10.2.12-h2	>= 10.2.12-h2
PAN-OS 10.1	None	All
Prisma Access	None	All

The Cal-CSIC recommends immediately upgrading to the latest version of PAN-OS.

For further information on applying mitigations please refer to Palo Alto Networks' community recommendations.

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] Palo Alto Networks. (2024, November 18). *CVE-2024-0012*. Palo Alto Networks. https://security.paloaltonetworks.com/CVE-2024-0012 Accessed November 18, 2024.
[2] Palo Alto Networks. (2024, November 18). *CVE-2024-9474*. Palo Alto Networks. https://security.paloaltonetworks.com/CVE-2024-9474 Accessed November 18, 2024.
[3] Palo Alto Networks. (2024, November 18). *CVE-2024-0012 / CVE-2024-9474*. Unit 42. https://unit42.paloaltonetworks.com/cve-2024-0012-cve-2024-9474/ Accessed November 18, 2024.
[4] Bleeping Computer. (2024, November 18). *Palo Alto Networks patches two firewall zero-days used in attacks*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/palo-alto-networks-patches-two-firewall-zero-days-used-in-attacks/ Accessed November 18, 2024.