CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

TLP:CLEAR
30 December 2024

PAN Firewall Denial of Service flaw Disabling PAN Firewalls

CVE-2024-3393 | DNS | DoS | Malicious Packet

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a Palo Alto's Network (PAN) firewall operating systems vulnerability, tracked as CVE-2024-3393 (CVSS 3.1 Score: 7.7).[1] This is a Denial of Service (DOS) vulnerability in the DNS Security feature of Palo Alto Networks PAN-OS software that allows an attacker to send malicious packets through the victim entity's firewall, causing it to reboot. Repeated attempts to trigger this condition will cause the firewall to enter maintenance mode, effectively taking the device offline.

This vulnerability has been exploited in attacks.[2] The exploitation is of low complexity and requires no elevated privileges, which possibly increases the likelihood that this vulnerability will be exploited in future attacks.

The Cal-CSIC recommends immediately updating to any of the following versions: PAN-OS 10.1.14-h8, PAN-OS 10.2.10-h12, PAN-OS 11.1.5, PAN-OS 11.2.3, and all later PAN-OS versions.

- *Note:* PAN-OS 11.0 reached the end of life (EOL) on November 17, 2024, so PAN does not intend to provide a fix for this release.

For further information please refer to PAN's advisory.

PAN Operating System upgrade guide to its latest version.

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 advisory is based on information obtained from trusted sources, such as NIST, the Australian government and reputable cybersecurity news websites.
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-2024-3393 PAN-OS: Firewall Denial of Service (DoS) in DNS Security Using a Specially Crafted Packet" https://security.paloaltonetworks.com/CVE-2024-3393; accessed 30 December 2024

[2] Bleeping Computer; "Hackers exploit DoS flaw to disable Palo Alto Networks firewalls" https://www.bleepingcomputer.com/news/security/hackers-exploit-dos-flaw-to-disable-palo-alto-networks-firewalls/; accessed 30 December 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.