CYBER ADVISORY

TLP:CLEAR

12 April 2024

PAN-OS Zero Day Vulnerability

CVE-2024-3400 | PAN-OS | Zero Day | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware a highly critical zero day vulnerability under active exploitation known as CVE-2024-3400.[1] The vulnerability affects Palo Alto Networks' PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1.[2,3] The command injection vulnerability lies within the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.[4]

The Cal-CSIC recommends immediately applying Palo Alto Networks recommended mitigations to avoid compromise. A patch has yet to be developed for this vulnerability.

For further information on applying recommended mitigations please refer to, CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway.

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] CISA; "Palo Alto Networks Releases Guidance for Vulnerability in PAN-OS, CVE-2024-3400;" https://cert.europa.eu/publications/security-advisories/2024-035/; accessed 12 April 2024
[2] The Stack; "Palo Alto Networks: CVSS 10 bug in Pan-OS is being exploited in the wild;" https://www.thestack.technology/palo-alto-networks-cvss-10-bug-in-pan-os-is-being-exploited-in-the-wild/; accessed 12 April 2024
[3] The Hacker News; "Zero-Day Alert: Critical Palo Alto Networks PAN-OS Flaw Under Active Attack;" https://thehackernews.com/2024/04/zero-day-alert-critical-palo-alto.html; accessed 12 April 2024
[4] National Vulnerability Database; "CVE-2024-3400 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-3400; accessed 12 April 2024