Assetnote Discovers Additional Critical Vulnerability (CVE-2025-0108) in Palo Alto Networks Management Interface PAN-OS

QUEENSLAND, AUSTRALIA, February 12, 2025 /EINPresswire.com/ -- - Assetnote, a Searchlight Cyber company, has identified a new critical vulnerability in the Palo Alto Networks management interface, known as PAN-OS.

Assetnote

This discovery comes shortly after Palo Alto Networks' November 18th advisory (CVE-2024-0012) regarding an authentication bypass that allowed attackers to gain PAN-OS administrator privileges, ultimately leading to RCE through a second vulnerability (CVE-2024-9474).

While Palo Alto Networks has released patches for the previously disclosed vulnerabilities, Assetnote's research team has discovered that fundamental architectural decisions in PAN-OS have left additional attack vectors exposed. This new finding represents a distinct, but related vulnerability that enables authentication bypass, allowing access to administrative functionalities that can allow for the takeover of the device.

"Our research reveals that while Palo Alto Networks's recent patches addressed the known vulnerabilities, the underlying architecture of PAN-OS contains additional security flaws within the same vulnerability class," said Shubham (Shubs) Shah, CTO and Co-Founder at Assetnote. "This highlights a critical need for vendors to consider holistic security architecture reviews when addressing security incidents. The new patch does fix the issue in PAN-OS 10.2.14, PAN-OS 11.0.7, PAN-OS 11.2.5, and all later PAN-OS versions."

Technical Impact:
The newly discovered vulnerability allows attackers to bypass authentication mechanisms.This represents a distinct security flaw from the recently patched vulnerabilities but stems from similar architectural design choices. "We disclosed this vulnerability immediately to Palo Alto so they could begin their remediation efforts," added Shubs. "Further investigation would likely have led to finding ways to escalate this to remote code execution, but we wanted to get this in the hands of Palo Alto as soon as possible given the recent CVE's."

Required Immediate Actions:
- Organizations must apply Palo Alto Networks' new security patch immediately upon release. More information can be found via Palo Alto's advisory number: PAN-273971 or through CVE-2025-0108.
- Allowlist IPs in the management interface to prevent this or similar vulnerabilities from being exploited over the internet.
- Implement enhanced monitoring for suspicious activity.
- Consider implementing additional network segmentation as a compensating control.

"This discovery underscores the importance of comprehensive security reviews and the growing need to understand how third-party products are extending customer attack surfaces," added Shubs. "We appreciate Palo Alto Networks's swift response to our disclosure and their commitment to addressing not just individual vulnerabilities, but also their architectural considerations."

You can read more in technical detail at https://slcyber.io/blog/nginx-apache-path-confusion-to-auth-bypass-in-pan-os/

About Assetnote, a Searchlight Cyber company:

Founded in 2018, Assetnote provides industry-leading attack surface management and adversarial exposure validation solutions, helping organizations identify and remediate security vulnerabilities before they can be exploited. Through continuous security testing and verification, Assetnote enables organizations to actionably defend their attack surface without noise. Assetnote customers receive security alerts and mitigations at the same time to disclosure to third-party vendors. In January 2025 Assetnote was acquired by Searchlight Cyber. Combined, the companies form a holistic platform for combating external threats through Continuous Threat Exposure Management. Visit assetnote.io and slcyber.io for more information or contact at press@assetnote.io

Sonia Awan
Outbloom Public Relations
soniaawan@outbloompr.net
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/785418039

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2025 Newsmatics Inc. All Right Reserved.