

HiveForce Labs

THREAT ADVISORY

 VULNERABILITY REPORT

PAN-OS Management Interface Flaw Exploited for Root-Level Code Execution

Date of Publication

October 15, 2026

Admiralty Code

A1

TA Number

TA2026303

Summary

First Seen: October 14, 2026

Affected Products: Palo Alto Networks PAN-OS (PA-Series, VM-Series, Panorama)

Impact: Palo Alto Networks has patched CVE-2026-0322, a high-severity code injection flaw (CVSS v4.0 8.6) in the PAN-OS management interface. It lets an authenticated attacker with network access execute arbitrary code with root privileges on PA-Series and VM-Series firewalls and on Panorama, and it works on default configurations. The flaw has been exploited in the wild as a zero-day, which makes patching and restricting management interface exposure urgent.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-0322	Palo Alto Networks PAN-OS Code Injection Vulnerability	Palo Alto Networks PAN-OS			

Vulnerability Details

#1

PAN-OS is the operating system that runs Palo Alto Networks PA-Series hardware and VM-Series virtual next-generation firewalls, along with the Panorama centralized management platform in both virtual and M-Series deployments, and its management interface serves as the administrative plane through which device configuration and security policy are controlled. CVE-2026-0322 is a high-severity remote code execution vulnerability in this management interface, classified as CWE-94 (Improper Control of Generation of Code) and rated 8.6 under CVSS v4.0.

#2

The flaw arises from improper control over code generation within the management interface, allowing an authenticated attacker with network access to the interface to inject code that executes with root privileges on the underlying firewall operating system. The attack carries low complexity, requires no user interaction and no special preconditions, and is exploitable on default configurations, although the scoring rates the privileges required as high, meaning the attacker must already hold an authenticated session on the device. Vulnerable builds span every supported release train from 10.2 through 12.2, while Cloud NGFW and Prisma Access are not affected.

#3

The flaw has been exploited in the wild as a zero-day targeting the PAN-OS management interface, and IP addresses linked to the exploit attempts have been released. Attribution, the start of the activity, and post-exploitation behavior have not been disclosed.

#4

Successful exploitation results in full compromise of the device's confidentiality, integrity, and availability, placing policy enforcement, configuration data, and traffic handling under attacker control and turning a perimeter security control into a foothold for deeper intrusion. Exposure is greatest where the management interface is reachable from internet addresses, and limiting access to a single jump box lowers but does not remove the risk.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-0322	Palo Alto Networks PAN-OS 12.2 (Before 12.2.4), 12.1 (Before 12.1.4-h12, 12.1.7-h8, 12.1.10-h2), 11.2 (Before 11.2.4-h22, 11.2.7-h21, 11.2.10-h15, 11.2.13-h3, 11.2.16), 11.1 (Before 11.1.4-h37, 11.1.6-h39, 11.1.7-h11, 11.1.10-h35, 11.1.13-h15, 11.1.16-h3), 10.2 (Before 10.2.7-h38, 10.2.10-h41, 10.2.13-h26, 10.2.16-h11, 10.2.18-h12) on PA-Series, VM-Series and Panorama	cpe:2.3:o:palo_alto_networks:pan-os:*.~.*.*.*.*.*.*	CWE-94

Recommendations



Upgrade to a Fixed PAN-OS Release Immediately: Upgrade affected PA-Series, VM-Series, and Panorama deployments to the fixed build for their release train: 12.2.4 or later on 12.2; 12.1.4-h12, 12.1.7-h8, or 12.1.10-h2 or later on 12.1; 11.2.4-h22, 11.2.7-h21, 11.2.10-h15, 11.2.13-h3, or 11.2.16 or later on 11.2; 11.1.4-h37, 11.1.6-h39, 11.1.7-h11, 11.1.10-h35, 11.1.13-h15, or 11.1.16-h3 or later on 11.1; and 10.2.7-h38, 10.2.10-h41, 10.2.13-h26, 10.2.16-h11, or 10.2.18-h12 or later on 10.2. Devices on older, unsupported PAN-OS versions must be moved to a supported fixed release, and Panorama should be prioritized alongside internet-reachable firewalls.



Lock Down Management Interface Access: Restrict the management interface to trusted internal IP addresses in line with the vendor's administrative access best practices, and preferably to a single hardened jump box that is the only system permitted to reach it. Remove management profiles that expose HTTPS or SSH management services on internet-facing or untrusted interfaces, since the vendor identifies internet-reachable management interfaces as the highest-risk condition for this flaw.



Apply Threat Prevention Signatures as Interim Coverage: No workaround exists, but organizations with a Threat Prevention subscription can enable Threat IDs 510046 and 510047, available from Applications and Threats content version 9159-10287 and later. The signatures only take effect when inbound management traffic is routed through a data-plane interface with a management profile, the certificate for inbound management traffic is replaced, that traffic is decrypted, and threat prevention is applied to it. The vendor describes this coverage as limited because attack variations may evade detection, so treat it strictly as a stopgap until patching is complete.



Hunt for and Block Published Indicators: Search management interface access logs, system and configuration logs, and perimeter telemetry for connections from the IP addresses listed in the IoCs section, and block them at upstream controls. Any historical hit against a management interface should be treated as a potential compromise and escalated for investigation.



Audit and Rotate Administrative Credentials: Because exploitation requires an authenticated session, review all local and externally authenticated administrator accounts for unfamiliar entries, unexpected role changes, or anomalous login sources, then rotate administrator passwords and API keys and enforce multi-factor authentication for management access. Credentials reused on other systems should be rotated as well.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1190</u> : Exploit Public-Facing Application	
Execution	<u>T1059</u> : Command and Scripting Interpreter	
Privilege Escalation	<u>T1068</u> : Exploitation for Privilege Escalation	



Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	66[.]42[.]72[.]14, 208[.]83[.]239[.]114, 149[.]248[.]47[.]234



Patch Link

<https://security.paloaltonetworks.com/CVE-2026-0322>



References

<https://security.paloaltonetworks.com/CVE-2026-0322>



What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of HivePro.

REPORT GENERATED ON

October 15, 2026 • 11:40 PM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com