Vulnerability Advisory

TLP: CLEAR

CAL-CSIC-2026-10-A-015

14 OCT 2026

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Authenticated Code Injection Vulnerability Found within Palo Alto Networks PAN-OS and Panorama

Arbitrary Code Injection	No User Interaction Required	Limited Exploitation	Security Fixes Available

The Cal-CSIC has become aware of a code injection vulnerability (CVE-2026-0322) affecting Palo Alto Networks PAN-OS and Panorama. PAN-OS provides firewall protection for network traffic, while Panorama centralizes firewall management. The vulnerability carries a CVSS 4.0 score of 8.6 for Internet-accessible management interfaces, or 8.5 when a jump box is the only system permitted to reach the interface.[1,2]

An authenticated attacker with high privileges and network access to the management interface could exploit the flaw to execute arbitrary code. Successful exploitation allows the attacker to run that code with root privileges on the firewall, potentially allowing access to sensitive data, unauthorized system changes, or service disruption. No special configuration or user interaction is required. PA-Series and VM-Series firewalls and Panorama virtual and M-Series systems are affected; Cloud NGFW and Prisma Access are unaffected.[1]

Palo Alto Networks has released maintenance-specific security fixes, with PAN-OS 11.2.16 scheduled for October 15, 2026. The vendor reports very limited exploitation targeting the management interface. No public proof of concept (PoC) was identified in the sources reviewed as of October 14, 2026. No known workaround exists; the vendor's Threat Prevention coverage is limited and requires specific traffic-inspection and decryption conditions.[3]

Cal-CSIC recommends that organizations operating affected firewalls or Panorama systems promptly apply an available fixed release for their maintenance line, following the vendor's upgrade guidance. Restrict management access to trusted internal addresses or a dedicated jump box immediately. Review the vendor's indicators of compromise and investigate suspicious management activity. For systems awaiting PAN-OS 11.2.16, verify release availability and maintain restricted management access until remediation is complete.[3]

For additional details regarding CVE-2026-0322, please use this link:

Palo Alto Networks Security Advisory:

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

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

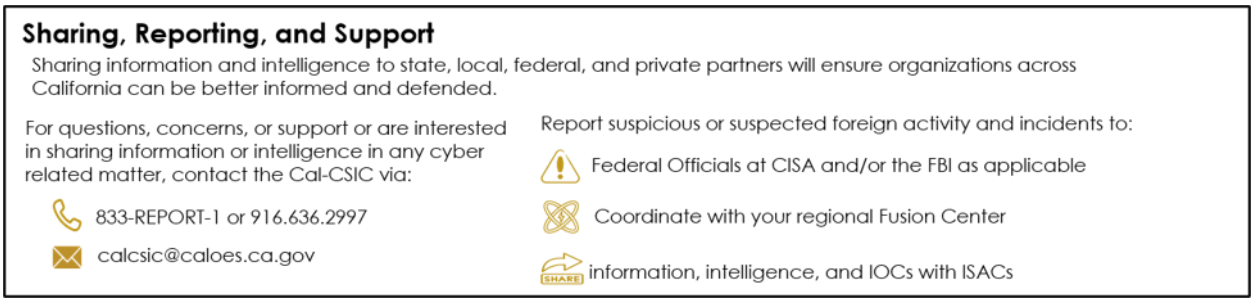
Affected Products and Versions

Product	Affected Version	Fixed Release
PAN-OS 12.2	12.2.0 through 12.2.3	12.2.4 or later
PAN-OS 12.1	12.1.0 through 12.1.4; hotfixes before 12.1.4-h12	12.1.4-h12
	12.1.5 through 12.1.7; hotfixes before 12.1.7-h8	12.1.7-h8
	12.1.8 through 12.1.10; hotfixes before 12.1.10-h2	12.1.10-h2
PAN-OS 11.2	11.2.0 through 11.2.4; hotfixes before 11.2.4-h22	11.2.4-h22
	11.2.5 through 11.2.7; hotfixes before 11.2.7-h21	11.2.7-h21
	11.2.8 through 11.2.10; hotfixes before 11.2.10-h15	11.2.10-h15
	11.2.11 through 11.2.13; hotfixes before 11.2.13-h3	11.2.13-h3
	11.2.14 through 11.2.15	11.2.16 or later (ETA 15 OCT 2026)
PAN-OS 11.1	11.1.0 through 11.1.4; hotfixes before 11.1.4-h37	11.1.4-h37
	11.1.5 through 11.1.6; hotfixes before 11.1.6-h39	11.1.6-h39
	11.1.7; hotfixes before 11.1.7-h11	11.1.7-h11
	11.1.8 through 11.1.10; hotfixes before 11.1.10-h35	11.1.10-h35
	11.1.11 through 11.1.13; hotfixes before 11.1.13-h15	11.1.13-h15
	11.1.14 through 11.1.16; hotfixes before 11.1.16-h3	11.1.16-h3

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Product	Affected Version	Fixed Release
PAN-OS 10.2	10.2.0 through 10.2.7; hotfixes before 10.2.7-h38	10.2.7-h38
	10.2.8 through 10.2.10; hotfixes before 10.2.10-h41	10.2.10-h41
	10.2.11 through 10.2.13; hotfixes before 10.2.13-h26	10.2.13-h26
	10.2.14 through 10.2.16; hotfixes before 10.2.16-h11	10.2.16-h11
	10.2.17 through 10.2.18; hotfixes before 10.2.18-h12	10.2.18-h12

Sharing, Reporting, and Support



References

[1] Palo Alto Networks via the CVE Program; "CVE-2026-0322 CNA Record"; https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2026/0xxx/CVE-2026-0322.json; accessed 14 October 2026

[2] Palo Alto Networks; "PAN-OS Documentation"; https://docs.paloaltonetworks.com/pan-os; accessed 14 October 2026

[3] Palo Alto Networks; "PAN-OS: Authenticated Remote Code Execution (RCE) in the Management Interface"; https://security.paloaltonetworks.com/CVE-2026-0322; accessed 14 October 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.