



# PAN-OS: Authenticated Admin Command Injection Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-0261
<b>State</b>	PUBLISHED
<b>Assigner</b>	palo_alto
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-13 19:17:02 UTC
<b>Updated</b>	2026-05-14 16:21:23 UTC
<b>Description</b>	Multiple command injection vulnerabilities in Palo Alto Networks PAN-OS® software enable an authenticated administrator

## Risk And Classification

**Primary CVSS:** v4.0 6.1 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:Amber

**EPSS:** 0.000810000 probability, percentile 0.237300000 (date 2026-05-17)

**Problem Types:** CWE-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	6.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:Amber
4.0	CNA	CVSS	6.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:Amber
4.0	CNA	CVSS	5.7	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:Amber

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/UA:member

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Palo Alto Networks</a>	<a href="#">Cloud NGFW</a>	unaffected All custom
CNA	<a href="#">Palo Alto Networks</a>	<a href="#">PAN-OS</a>	affected 12.1.0 12.1.7, 12.1.4-h5 custom
CNA	<a href="#">Palo Alto Networks</a>	<a href="#">PAN-OS</a>	affected 11.2.0 11.2.12, 11.2.10-h6, 11.2.7-h13, 11.2.4-h17 custom
CNA	<a href="#">Palo Alto Networks</a>	<a href="#">PAN-OS</a>	affected 11.1.0 11.1.15, 11.1.13-h5, 11.1.10-h25, 11.1.7-h6, 11.1.6-h32, 11.1.4-h33 custom
CNA	<a href="#">Palo Alto Networks</a>	<a href="#">PAN-OS</a>	affected 10.2.0 10.2.18-h6, 10.2.16-h7, 10.2.13-h21, 10.2.10-h36, 10.2.7-h34 custom
CNA	<a href="#">Palo Alto Networks</a>	<a href="#">Prisma Access</a>	unaffected All custom

### References

Reference	Source	Link	Tags
<a href="#">security.paloaltonetworks.com/CVE-2026-0261</a>	<a href="mailto:psirt@paloaltonetworks.com">psirt@paloaltonetworks.com</a>	<a href="#">security.paloaltonetworks.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Palo Alto Networks thanks our internal security research teams for discovering and reporting this issue. (en)

## Additional Advisory Data

Source	Time	Event
CNA	2026-05-13T16:00:00.000Z	Initial publication.

### Solutions

**CNA:** VERSION MINOR VERSION SUGGESTED SOLUTION Cloud NGFW No action needed. PAN-OS 12.1 12.1.5 through 12.1.6 Upgrade to 12.1.7 or later. 12.1.2 through 12.1.4-h\* Upgrade to 12.1.4-h5 or 12.1.7 or later. PAN-OS 11.2 11.2.11 or later Upgrade to 11.2.12 or later. 11.2.8 through 11.2.10-h\* Upgrade to 11.2.10-h6 or 11.2.12 or later. 11.2.5 through 11.2.7-h\* Upgrade to 11.2.7-h13 or 11.2.12 or later. 11.2.0 through 11.2.4-h\* Upgrade to 11.2.4-h17 or 11.2.12 or later. PAN-OS 11.1 11.1.14 or later Upgrade to 11.1.15 or later. 11.1.11 through 11.1.13-h\* Upgrade to 11.1.13-h5 or 11.1.15 or later. 11.1.8 through 11.1.10-h\* Upgrade to 11.1.10-h25 or 11.1.15 or later. 11.1.7 through 11.1.7-h\* Upgrade to 11.1.7-h6 or 11.1.15 or later. 11.1.5 through 11.1.6-h\* Upgrade to 11.1.6-h32 or 11.1.15 or later. 11.1.0 through 11.1.4-h\* Upgrade to 11.1.4-h33 or 11.1.15 or later. PAN-OS 10.2 10.2.17 through 10.2.18-h\* Upgrade to 10.2.18-h6 or later. 10.2.14 through 10.2.16-h\* Upgrade to 10.2.16-h7 or 10.2.18-h6 or later. 10.2.11 through 10.2.13-h\* Upgrade to 10.2.13-h21 or 10.2.18-h6 or later. 10.2.8 through 10.2.10-h\* Upgrade to 10.2.10-h36 or 10.2.18-h6 or later. 10.2.0 through 10.2.7-h\* Upgrade to 10.2.7-h34 or 10.2.18-h6 or later. All older Upgrade to a supported fixed version. unsupported PAN-OS versions Prisma Access No action needed.

### Workarounds

**CNA:** The vast majority of firewalls already follow Palo Alto Networks' and industry best practices. However, if you have not already, we strongly recommend that you secure access to your management interface according to our best practice deployment guidelines (<https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431>). Specifically, you should restrict management interface access to only trusted internal IP addresses. Review information about how to secure management access to your Palo Alto Networks firewalls: \* Palo Alto Networks LIVEcommunity article: <https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431> \* Palo Alto Networks official and detailed technical documentation: <https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices> Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat IDs 510017, 510018 and 510024 and can detect attacks for this vulnerability by enabling Threat IDs 510021, 510025 and 510026 (from Applications and Threats content version 9100-10044 and later). For these Threat IDs to protect against attacks for this vulnerability: \* Route incoming traffic for the MGT port through a DP port (<https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices#id59206398-3dab-4b2f-9b4b-7ea500d036ba>), e.g., enabling management profile on a DP interface for management access. \* Replace the

Certificate for Inbound Traffic Management (<https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices#id112f7714-8995-4496-bbf9-781e63dec71c>). \* Decrypt inbound traffic to the management interface (<https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices#idb82587-17a2-42b4-9245-d3714e1e13a2>) so the firewall can inspect it (<https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices#idb82587-17a2-42b4-9245-d3714e1e13a2>). \* Enable threat prevention on the inbound traffic to management services.

Exploits

**CNA:** Palo Alto Networks is not aware of any malicious exploitation of these issues.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)