PAN-OS: Authentication Bypass with Cloud Authentication Service (CAS) enabled

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-0265
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 18:16:14 UTC
Updated	2026-05-13 18:17:47 UTC
Description	An authentication bypass vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with r

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:U/V:D/RE:M/U:Red

EPSS: 0.000760000 probability, percentile 0.226300000 (date 2026-05-15)

Problem Types: CWE-347 | CWE-347 CWE-347 Improper Verification of Cryptographic Signature

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	7.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	7.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	2.7	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

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:P/PR:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:U/V:D/RE:M/U:Red

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Palo Alto Networks	Cloud NGFW	unaffected All custom
CNA	Palo Alto Networks	PAN-OS	affected 12.1.0 12.1.7, 12.1.4-h5 custom
CNA	Palo Alto Networks	PAN-OS	affected 11.2.0 11.2.12, 11.2.10-h6, 11.2.7-h13, 11.2.4-h17 custom
CNA	Palo Alto Networks	PAN-OS	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	Palo Alto Networks	PAN-OS	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	Palo Alto Networks	Prisma Access	unaffected All custom

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0265	psirt@paloaltonetworks.com	security.paloaltonetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Palo Alto Networks thanks Harsh Jaiswal from Hacktron AI and 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 RANGE 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 haven’t already, we strongly recommend that you secure access to your management interface according to our best practice deployment guidelines. Specifically, you should restrict access to the management interface to only trusted internal IP addresses to prevent external access from the internet. 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 more detailed technical documentation: https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices To temporarily mitigate this issue, customers can disable the Cloud Authentication Service (CAS) by changing the associated authentication profile to SAML, RADIUS, or other supported authentication methods. Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat ID 510008 from Applications and Threats content version 9100-10044 and later. Threat ID 510008 depends on features present in PAN-OS 11.2 and above. To ensure the Threat ID provides effective protection against this vulnerability, follow these steps: * 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. * Ensure that vulnerability protection security profile is applied to your GlobalProtect interface (https://live.paloaltonetworks.com/t5/globalprotect-articles/applying-vulnerability-protection-to-globalprotect-interfaces/ta-p/340184). * Replace the default 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 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#idbbd82587-17a2-42b4-9245-d3714e1e13a2). * Enable Threat Prevention on the inbound traffic to management services.

Exploits

CNA: Palo Alto Networks is not aware of any malicious exploitation of this issue.

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