PAN-OS: Stored Cross-Site Scripting (XSS) Vulnerability in the Web Interface

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

Summary

CVE	CVE-2026-0256
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 19:17:00 UTC
Updated	2026-05-14 16:21:23 UTC
Description	A stored cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS® software enables a malicious authenticate

Risk And Classification

Primary CVSS: v4.0 4.4 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:H/VA:N/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:Amber

EPSS: 0.000430000 probability, percentile 0.132640000 (date 2026-05-18)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	4.4	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:H/VA:N/SC:N/SI:N/S
4.0	CNA	CVSS	4.4	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:H/VA:N/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

Passive

Confidentiality

Low

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:H/VA:N/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:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Palo Alto Networks	Cloud NGFW	unaffected All custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 12.1.0 12.1.7 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 11.2.0 11.2.12 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 11.1.0 11.1.15 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 10.2.0 10.2.18-h6 custom	Not specified
CNA	Palo Alto Networks	Prisma Access	unaffected All custom	Not specified

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0256	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 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: Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat ID 510020 (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#idbbd82587-17a2-42b4-9245-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#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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**