PAN-OS: Improper Neutralization of Input in the Management Web Interface

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-4615
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-09 19:15:43 UTC
Updated	2026-04-01 01:16:39 UTC
Description	An improper input neutralization vulnerability in the management web interface of the Palo Alto Networks PAN-OS® softwa

Risk And Classification

Primary CVSS: v4.0 5.5 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/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

Problem Types: CWE-83 | CWE-83 CWE-83 Improper Neutralization of Script in Attributes in a Web Page

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	5.5	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	5.4	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	5.5	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/S
3.1	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

High

User Interaction

None

Confidentiality

None

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:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

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	unaffected 12.1.0 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 11.2.0 11.2.8 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 11.1.0 11.1.4-h27 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 10.2.0 10.2.17 custom	Not specified
CNA	Palo Alto Networks	Prisma Access	unaffected All custom	Not specified

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVEN-2025-4615	psirt@paloaltonetworks.com	security.paloaltonetworks.com	Vendor Advisory
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: Visa Inc. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-19T21:55:00.000Z	Updated fix version for 11.1.0.
CNA	2025-11-11T19:15:00.000Z	Updated Fixed Software Versions
CNA	2025-10-08T16:00:00.000Z	Initial Publication
CNA	2026-04-01T00:15:00.000Z	Updated exploit maturity

Solutions

CNA: VERSION MINOR VERSION SUGGESTED SOLUTION Cloud NGFW All No action needed. PAN-OS 12.1 No action needed. PAN-OS 11.2 11.2.0 through 11.2.7 Upgrade to 11.2.8 or later. PAN-OS 11.1 11.1.0 through 11.1.4 Upgrade to 11.1.4-h27 or 11.1.6-h21 or 11.1.10-h7 or later. 11.1.4 through 11.1.6 Upgrade to 11.1.6-h21 or 11.1.10-h7 or later. 11.1.8 through 11.1.10 Upgrade to 11.1.10-h7 or later. PAN-OS 10.2 10.2.0 through 10.2.16 Upgrade to 10.2.17 or later. All older Upgrade to a supported fixed version. unsupported PAN-OS versions Prisma Access All No action needed.

Workarounds

CNA: No known workarounds exist for this issue.

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.