PAN-OS: Reflected Cross-Site Scripting (XSS) Vulnerability in GlobalProtect Gateway and Portal

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-0133
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-14 19:15:51 UTC
Updated	2026-04-03 00:16:03 UTC
Description	A reflected cross-site scripting (XSS) vulnerability in the GlobalProtect™ gateway and portal features of Palo Alto Networks

Risk And Classification

Primary CVSS: v4.0 2.7 LOW from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/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:N/AU:N/R:U/V:D/RE:M/U:Amber

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	2.7	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	1.2	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	2.7	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/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:N/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	affected All 11.2.8 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 11.2.0 11.2.7 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 11.1.0 11.1.6-h14 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 10.2.0 10.2.16-h1 custom	Not specified
CNA	Palo Alto Networks	PAN-OS	affected 10.1.0 custom	Not specified
CNA	Palo Alto Networks	Prisma Access	affected All custom	Not specified

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2025-0133	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: XBOW (en)

Additional Advisory Data

Source	Time	Event

CNA	2025-07-09T16:00:00.000Z	Added fix version for PAN-OS 10.2.
CNA	2025-07-04T06:30:00.000Z	Added Releases with the Software Fix, Updated Recommended Content Version, and Added Guidanc
CNA	2025-06-18T19:15:00.000Z	Changed Content Version for Mitigation and Updated Version ETAs
CNA	2025-05-21T20:30:00.000Z	Removed Cloud NGFW from Affected Products
CNA	2025-05-21T00:00:00.000Z	Removed Prisma Access from Affected Products.
CNA	2025-05-15T20:00:00.000Z	Changed Expected Fix Release for PAN-OS 11.2
CNA	2025-05-15T19:00:00.000Z	Added Prisma Access and Cloud NGFW to Affected Products.
CNA	2025-05-14T16:00:00.000Z	Initial Publication

Solutions

CNA: VERSION MINOR VERSION SUGGESTED SOLUTION PAN-OS 11.2 11.2.0 through 11.2.4 Upgrade to 11.2.4-h9 or later 11.2.5 through 11.2.6 Upgrade to 11.2.7 or later PAN-OS 11.1 11.1.0 through 11.1.6 Upgrade to 11.1.6-h14 or later 11.1.7 through 11.1.10 Upgrade to 11.1.10-h1 or later PAN-OS 10.2 10.2.0 through 10.2.16 Upgrade to 10.2.16-h1 or later PAN-OS 10.1 10.1.0 through 10.1.14 Upgrade to 10.2.16-h1 or later All other older unsupported PAN-OS versions Upgrade to a supported fixed version PAN-OS 10.1 is in L (https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-life-policy)imited Support (https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-life-policy) and reaches Software EOL (https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-life-summary)in March 2026. https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-life-policy

Workarounds

CNA: Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat ID 510003 and 510004 from Applications and Threats content version 8995. For all Cloud NGFW, PAN-OS, and Prisma Access deployments, it is crucial to ensure that Vulnerability Protection profiles are explicitly applied to the security rules that process traffic from GlobalProtect interfaces. This ensures the Threat Prevention signatures are actively enforced. For detailed guidance on applying Vulnerability Protection to GlobalProtect interfaces, please refer to: https://live.paloaltonetworks.com/t5/globalprotect-articles/applying-vulnerability-protection-to-globalprotect-interfaces/ta-p/340184. You can also disable Clientless VPN to reduce impact in the event of exploitation, though this will not block the exploit in it's entirety. For more information, review the security advisory PAN-SA-2025-0005 (https://security.paloaltonetworks.com/PAN-SA-2025-0005). Previous versions of this advisory have listed the recommended content version as 8970 and 8990. We now recommend 8995 as it has the latest updates to the signatures to cover additional exploit variants.

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.

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