CVE-2025-0133 PAN-OS: Reflected Cross-Site Scripting (XSS) Vulnerability in GlobalProtect Gateway and Portal

Urgency MODERATE

Severity 2 · LOW

Exploit Maturity **POC**	Response Effort **N/A**	Recovery **USER**	Value Density **DIFFUSE**
Attack Vector **NETWORK**	Attack Complexity **LOW**	Attack Requirements **NONE**	Automatable **NO**
User Interaction **ACTIVE**	Product Confidentiality **NONE**	Product Integrity **LOW**	Product Availability **NONE**
Privileges Required **NONE**	Subsequent Confidentiality **NONE**	Subsequent Integrity **NONE**	Subsequent Availability **NONE**

CVE JSON CSAF

Published **2025-05-14**

Updated **2025-07-09**

Reference **PAN-287002**

Discovered **externally**

Description

A reflected cross-site scripting (XSS) vulnerability in the GlobalProtect™ gateway and portal features of Palo Alto Networks PAN-OS® software enables execution of malicious JavaScript in the context of an authenticated Captive Portal user's browser when they click on a specially crafted link. The primary risk is phishing attacks that can lead to credential theft—particularly if you enabled Clientless VPN.

There is no availability impact to GlobalProtect features or GlobalProtect users. Attackers cannot use this vulnerability to tamper with or modify contents or configurations of the GlobalProtect portal or gateways. The integrity impact of this vulnerability is limited to enabling an attacker to create phishing and credential-stealing links that appear to be hosted on the GlobalProtect portal.

For GlobalProtect users with Clientless VPN enabled, there is a limited impact on confidentiality due to inherent risks of Clientless VPN that facilitate credential theft. You can read more about this risk in the informational bulletin PAN-SA-2025-0005. There is no impact to confidentiality for GlobalProtect users if you did not enable (or you disable) Clientless VPN.

Product Status

Versions	Affected	Unaffected
Cloud NGFW	All	None (See Mitigations and Workarounds)
PAN-OS 11.2	< 11.2.4-h9 < 11.2.7	>= 11.2.4-h9 >= 11.2.7
PAN-OS 11.1	< 11.1.6-h14 < 11.1.10-h1	>= 11.1.6-h14 >= 11.1.10-h1
PAN-OS 10.2	< 10.2.16-h1	>= 10.2.16-h1
PAN-OS 10.1	All	None
Prisma Access	All	None (See Mitigations and Workarounds)

Required Configuration for Exposure

This issue is applicable only to PAN-OS firewall configurations with an enabled GlobalProtect gateway or portal.

Severity: LOW, Suggested Urgency: MODERATE

Without Clientless VPN
LOW - CVSS-BT: 2.0 /CVSS-B: 5.1
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/AU:N/R:U/V:D/U:Amber)

With Clientless VPN enabled, there are inherent risks that facilitate credential stealing (enumerated in PAN-SA-2025-0005).
MEDIUM - CVSS-BT: 5.5 /CVSS-B: 6.9
(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:P/S:N/AU:N/R:U/V:D/RE:M/U:Amber)

Exploitation Status

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

Weakness Type and Impact

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

CAPEC-591 Reflected XSS

Solution

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 Limited Support and reaches Software EOL in March 2026.

Workarounds and Mitigations

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.

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.

Acknowledgments

Palo Alto Networks thanks XBOW for discovering and reporting this issue.

CPEs

cpe:2.3:o:paloaltonetworks:pan-os:11.2.6:*:*:*:*:*:*:*

cpe:2.3:o:paloaltonetworks:pan-os:11.2.5:*:*:*:*:*:*:*

cpe:2.3:o:paloaltonetworks:pan-os:11.2.4:*:*:*:*:*:*:*

cpe:2.3:o:paloaltonetworks:pan-os:11.2.3:*:*:*:*:*:*:*

cpe:2.3:o:paloaltonetworks:pan-os:11.2.2:*:*:*:*:*:*:*

cpe:2.3:o:paloaltonetworks:pan-os:11.2.1:*:*:*:*:*:*:*

cpe:2.3:o:paloaltonetworks:pan-os:11.2.0:*:*:*:*:*:*:*

cpe:2.3:o:paloaltonetworks:pan-os:11.1.9:*:*:*:*:*:*:*

cpe:2.3:o:paloaltonetworks:pan-os:11.1.8:*:*:*:*:*:*:*

cpe:2.3:o:paloaltonetworks:pan-os:11.1.6:*:*:*:*:*:*:*

Show More

CPE Applicability

- cpe:2.3:o:palo_alto_networks:cloud_ngfw:*:*:*:*:*:*:*:* **is vulnerable** from (including)all
- **or**
  - cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.2.0 **and** up to (excluding)11.2.7
  - **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.2.4 **and** up to (excluding)11.2.4-h9
  - **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.1.10 **and** up to (excluding)11.1.10-h1
  - **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.1.6 **and** up to (excluding)11.1.6-h14
  - **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)10.2.16 **and** up to (excluding)10.2.16-h1
  - **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)10.1.0
- **or**
  - cpe:2.3:o:palo_alto_networks:prisma_access:*:*:*:*:*:*:*:* **is vulnerable** from (including)all

Timeline

2025-07-09 Added fix version for PAN-OS 10.2.

2025-07-04 Added Releases with the Software Fix, Updated Recommended Content Version, and Added Guidance for Prisma Access.

2025-06-18 Changed Content Version for Mitigation and Updated Version ETAs

2025-05-21 Removed Cloud NGFW from Affected Products

2025-05-21 Removed Prisma Access from Affected Products.

2025-05-15 Changed Expected Fix Release for PAN-OS 11.2

2025-05-15 Added Prisma Access and Cloud NGFW to Affected Products.

2025-05-14 Initial Publication