PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities

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

Summary

CVE	CVE-2026-0257
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 19:17:01 UTC
Updated	2026-05-13 19:17:01 UTC
Description	Authentication bypass vulnerabilities in the GlobalProtect portal and gateway of Palo Alto Networks PAN-OS® software allo

Risk And Classification

Primary CVSS: v4.0 4.7 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:H/SI:H/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:A/V:D/RE:M/U:Amber

Problem Types: CWE-565 | CWE-565 CWE-565 Reliance on Cookies without Validation and Integrity Checking

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	4.7	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:H/SI:H/S
4.0	CNA	CVSS	4.7	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:H/SI:H/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:H/SI:H/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:A/V:D/RE:M/U:Amber

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-h6 custom
CNA	Palo Alto Networks	PAN-OS	affected 11.2.0 11.2.12, 11.2.10-h7, 11.2.7-h14, 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	affected 10.2.0 10.2.10-h36 custom
CNA	Palo Alto Networks	Prisma Access	affected 11.2.0 11.2.7-h13 custom

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0257	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 SUGGESTED SOLUTION Cloud NGFW All 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-h6 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-h7 or 11.2.12 or later. 11.2.5 through 11.2.7-h* Upgrade to 11.2.7-h14 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 or 10.2.18-h6 or later. 10.2.14 through 10.2.16-h* Upgrade to 10.2.16-h7 or 10.2.18 or later. 10.2.11 through 10.2.13-h* Upgrade to 10.2.13-h21 or 10.2.18 or later. 10.2.8 through 10.2.10-h* Upgrade to 10.2.10-h36 or 10.2.18 or later. 10.2.0 through 10.2.7-h* Upgrade to 10.2.7-h34 or 10.2.18 or later. All older Upgrade to a supported fixed version. unsupported PAN-OS versions Prisma Access 10.2 10.2.0 through 10.2.10-h* Upgrade to 10.2.10-h36 or later. Prisma Access 11.2 11.2.0 through 11.2.7-h* Upgrade to 11.2.7-h13 or later. Note: With this fix, if the firewall is configured to use an authentication override cookie for the GlobalProtect Portal or Gateway, it will regenerate the cookie using a more secure method. Therefore, GP users will need to re-authenticate after a PAN-OS upgrade, even if a valid cookie is present. This is a one time requirement. Once they re-authenticate after the upgrade, the authentication override cookie and its validity will work as they do today.

Workarounds

CNA: Customers can mitigate the risk of this issue by taking any of the following actions: * Use a dedicated certificate for Authentication Override cookies: Generate a new certificate exclusively for authentication override cookies and store it securely. Do not reuse the portal or gateway certificate, and do not share this certificate with other features or users. * Disable Authentication Override: Uncheck the Authentication Override options (for generating and accepting cookies) in the GlobalProtect portal and gateway configuration.

Exploits

CNA: Palo Alto Networks is not aware of any malicious exploitation of these issues.

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