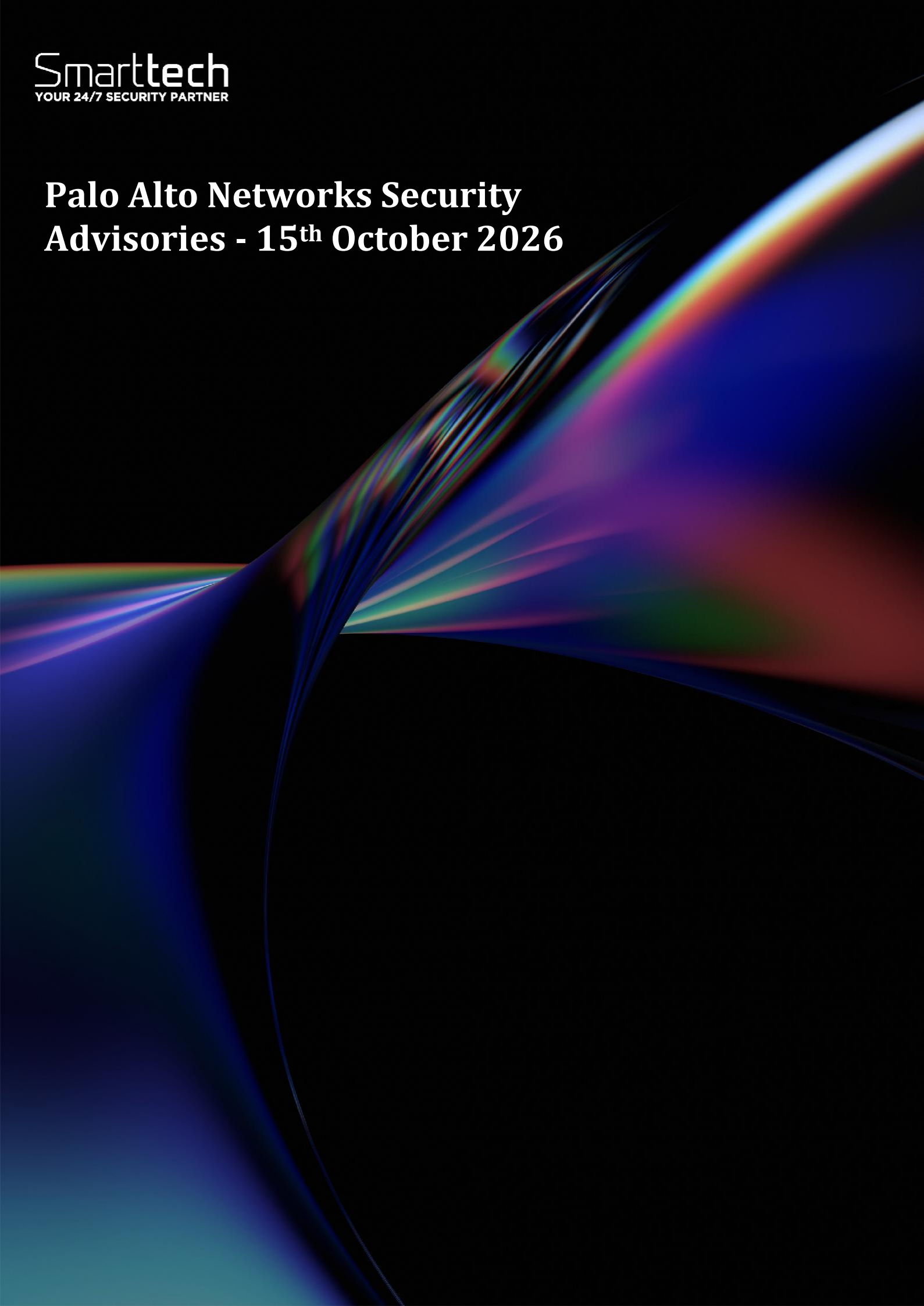


Palo Alto Networks Security Advisories - 15th October 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	176
Authors	Gabriel Gheorghiu < gabriel.gheorghiu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-15
Issue Date	2026-10-15

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.

Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Palo Alto Networks has disclosed multiple security vulnerabilities affecting PAN-OS, Cloud NGFW, Prisma Access, Panorama, GlobalProtect App, Prisma Browser, Cortex XSOAR, Cortex XSIAM, and Checkov by Prisma Cloud. The disclosed issues include authenticated remote code execution, command injection, denial-of-service, cross-site scripting, improper input handling, local privilege escalation, path traversal, server-side request forgery (SSRF), and Chromium-based vulnerabilities. The highest published severity in this release is CVSS 8.6 and no critical vulnerabilities were reported.

RISK:

Government:

- Large and medium government entities: High
- Small government entities: Medium

Businesses:

- Large and medium business entities: High
- Small business entities: Medium

TECHNICAL SUMMARY:

CVE-2026-0322 PAN-OS: Authenticated Remote Code Execution in the Management Interface CVSSv4.0 Base Score: 8.6

A remote code execution (RCE) vulnerability in the management interface of Palo Alto Networks PAN-OS® software enables an authenticated attacker with network access to execute arbitrary code with root privileges on the firewall.

The vulnerability impacts PAN-OS running on PA-Series and VM-Series firewalls, as well as Panorama (M-Series and virtual appliances). The risk associated with this vulnerability can be significantly reduced by restricting management interface access to trusted internal IP addresses and applying the vendor-provided security updates.

Affected Products:

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.2	< 12.2.4	>= 12.2.4
PAN-OS 12.1	< 12.1.4-h12 < 12.1.7-h8 < 12.1.10-h2	>= 12.1.4-h12 >= 12.1.7-h8 >= 12.1.10-h2
PAN-OS 11.2	< 11.2.4-h22 < 11.2.7-h21 < 11.2.10-h15 < 11.2.13-h3 < 11.2.16	>= 11.2.4-h22 >= 11.2.7-h21 >= 11.2.10-h15 >= 11.2.13-h3 >= 11.2.16 (ETA: 10/15)
PAN-OS 11.1	< 11.1.4-h37 < 11.1.6-h39 < 11.1.7-h11 < 11.1.10-h35 < 11.1.13-h15 < 11.1.16-h3	>= 11.1.4-h37 >= 11.1.6-h39 >= 11.1.7-h11 >= 11.1.10-h35 >= 11.1.13-h15 >= 11.1.16-h3
PAN-OS 10.2	< 10.2.7-h38 < 10.2.10-h41 < 10.2.13-h26 < 10.2.16-h11 < 10.2.18-h12	>= 10.2.7-h38 >= 10.2.10-h41 >= 10.2.13-h26 >= 10.2.16-h11 >= 10.2.18-h12
Prisma Access	None	None

Solution:

Upgrade affected PAN-OS systems to the vendor-recommended fixed versions listed in the Affected Products table. Restrict access to the management interface to trusted internal IP addresses and review administrative access controls to minimize exposure.

CVE-2026-0321 PAN-OS: Denial of Service Vulnerabilities in Network Services CVSSv4.0 Base Score: 6.6

Denial of service vulnerabilities in Palo Alto Networks PAN-OS® software allow an unauthenticated attacker with network access to cause a denial of service (DoS) condition by sending specially crafted network traffic to or through a data plane interface. Repeated attempts to trigger this condition resulted in the firewall entering maintenance mode.

Cloud NGFW and Panorama are not affected by this vulnerability.

Affected Products:

Versions	Affected	Unaffected
----------	----------	------------

Cloud NGFW	None	All
PAN-OS 12.2	< 12.2.4	>= 12.2.4
PAN-OS 12.1	< 12.1.4-h12 < 12.1.7-h8 < 12.1.10-h2	>= 12.1.4-h12 >= 12.1.7-h8 >= 12.1.10-h2
PAN-OS 11.2	< 11.2.4-h22 < 11.2.7-h21 < 11.2.10-h15 < 11.2.13-h3 < 11.2.16	>= 11.2.4-h22 >= 11.2.7-h21 >= 11.2.10-h15 >= 11.2.13-h3 >= 11.2.16 (ETA: 10/15)
PAN-OS 11.1	< 11.1.4-h37 < 11.1.6-h39 < 11.1.7-h11 < 11.1.10-h35 < 11.1.13-h15 < 11.1.16-h3	>= 11.1.4-h37 >= 11.1.6-h39 >= 11.1.7-h11 >= 11.1.10-h35 >= 11.1.13-h15 >= 11.1.16-h3
PAN-OS 10.2	< 10.2.7-h38 < 10.2.10-h41 < 10.2.13-h26 < 10.2.16-h11 < 10.2.18-h12	= 10.2.7-h38 >= 10.2.10-h41 >= 10.2.13-h26 >= 10.2.16-h11 >= 10.2.18-h12
Prisma Access 12.1	< 12.1.7-h8*	>= 12.1.7-h8*
Prisma Access 11.2	< 11.2.7-h21*	>= 11.2.7-h21*
Prisma Access 10.2	< 10.2.10-h41*	>= 10.2.10-h41*

Solution:

Upgrade affected PAN-OS systems to the fixed versions identified in the Affected Products table and apply vendor-recommended security updates.

CVE-2026-0320 PAN-OS: Authenticated Admin Command Injection Vulnerability CVSSv4.0 Base Score: 6.1

A command injection vulnerability in Palo Alto Networks PAN-OS® software enables an authenticated administrator to bypass system restrictions and run arbitrary commands as a root user. To be able to exploit this issue, the user must have access to the PAN-OS management interface.

The security risk posed by this issue is significantly minimized by restricting access to the management interface to only trusted internal IP addresses

This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series).

Cloud NGFW and Prisma® Access are not affected by this vulnerability.

Affected Products:

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.2	< 12.2.4	>= 12.2.4
PAN-OS 12.1	< 12.1.4-h12 < 12.1.7-h8 < 12.1.10-h2	>= 12.1.4-h12 >= 12.1.7-h8 >= 12.1.10-h2
PAN-OS 11.2	< 11.2.4-h22 < 11.2.7-h21 < 11.2.10-h15 < 11.2.13-h3 < 11.2.16	>= 11.2.4-h22 >= 11.2.7-h21 >= 11.2.10-h15 >= 11.2.13-h3 >= 11.2.16 (ETA: 10/15)
PAN-OS 11.1	< 11.1.4-h37 < 11.1.6-h39 < 11.1.7-h11 < 11.1.10-h35 < 11.1.13-h15 < 11.1.16-h3	>= 11.1.4-h37 >= 11.1.6-h39 >= 11.1.7-h11 >= 11.1.10-h35 >= 11.1.13-h15 >= 11.1.16-h3
PAN-OS 10.2	< 10.2.7-h38 < 10.2.10-h41 < 10.2.13-h26 < 10.2.16-h11 < 10.2.18-h12	>= 10.2.7-h38 >= 10.2.10-h41 >= 10.2.13-h26 >= 10.2.16-h11 >= 10.2.18-h12
Prisma Access	None	All

Solution:

Upgrade affected PAN-OS systems to the fixed versions identified in the Affected Products table and apply vendor-recommended security updates.

CVE-2026-0313 Cortex XSOAR: OS Command Injection Vulnerability CVSSv4.0 Base Score: 6.1

A command injection vulnerability in Palo Alto Networks Cortex XSOAR and Cortex XSIAM OS Query content pack enables an authenticated administrator to execute arbitrary OS commands on remote endpoints.

Affected Products:

Versions	Affected	Unaffected
Cortex XSIAM OS Query	< 1.0.17	>= 1.0.17

Cortex XSOAR OS Query	< 1.0.17	>= 1.0.17
-----------------------	----------	-----------

Solution:

Upgrade Cortex XSOAR and Cortex XSIAM OS Query content packs to version 1.0.17 or later as specified in the Product Status table.

CVE-2026-0315 GlobalProtect App: Local Privilege Escalation Vulnerability on macOS CVSSv4.0 Base Score: 5.9

A local privilege escalation vulnerability in the Palo Alto Networks GlobalProtect™ app enables a local user to escalate their privileges to root on macOS. This enables a non-administrative user to execute arbitrary commands with administrative privileges.

The GlobalProtect app on Linux, Windows, iOS, Android and Chrome OS is not affected by this vulnerability.

Product Status:

Versions	Affected	Unaffected
GlobalProtect App	None on Linux None on Windows None on iOS None on Android None on ChromeOS	All on Linux All on Windows All on iOS All on Android All on ChromeOS
GlobalProtect App 6.3	< 6.3.3-h16 (6.3.3-1199) on macOS	>= 6.3.3-h16 (6.3.3-1199) on macOS
GlobalProtect App 6.2	< 6.2.8-h15 (6.2.8-1084) on macOS	>= 6.2.8-h15 (6.2.8-1084) on macOS

Solution:

Upgrade affected GlobalProtect App installations to the fixed versions identified in the Product Status table.

CVE-2026-0319 PAN-OS: Improper Input Handling Vulnerability CVSSv4.0 Base Score: 4.9

An improper input handling vulnerability in the GlobalProtect™ gateway of Palo Alto Networks PAN-OS software enables an authenticated user to establish a GlobalProtect session using the identity of another user.

Cloud NGFW and Panorama are not affected by this vulnerability.

Product Status:

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.2	< 12.2.4	>= 12.2.4
PAN-OS 12.1	< 12.1.4-h12 < 12.1.7-h8 < 12.1.10-h2	>= 12.1.4-h12 >= 12.1.7-h8 >= 12.1.10-h2
PAN-OS 11.2	< 11.2.4-h22 < 11.2.7-h21 < 11.2.10-h15 < 11.2.13-h3 < 11.2.16	>= 11.2.4-h22 >= 11.2.7-h21 >= 11.2.10-h15 >= 11.2.13-h3 >= 11.2.16 (ETA: 10/15)
PAN-OS 11.1	< 11.1.4-h37 < 11.1.6-h39 < 11.1.7-h11 < 11.1.10-h35 < 11.1.13-h15 < 11.1.16-h3	>= 11.1.4-h37 >= 11.1.6-h39 >= 11.1.7-h11 >= 11.1.10-h35 >= 11.1.13-h15 >= 11.1.16-h3
PAN-OS 10.2	< 10.2.7-h38 < 10.2.10-h41 < 10.2.13-h26 < 10.2.16-h11 < 10.2.18-h12	>= 10.2.7-h38 >= 10.2.10-h41 >= 10.2.13-h26 >= 10.2.16-h11 >= 10.2.18-h12
Prisma Access 12.1	< 12.1.7-h8	>= 12.1.7-h8
Prisma Access 11.2	< 11.2.7-h21	>= 11.2.7-h21
Prisma Access 10.2	< 10.2.10-h41	>= 10.2.10-h41

Solution:

Upgrade affected PAN-OS systems to the fixed versions identified in the Product Status table.

CVE-2026-0318 PAN-OS: Denial of Service (DoS) on Panorama **CVSSv4.0 Base Score: 4.6**

A stack-based buffer overflow vulnerability in the log processing functionality of Palo Alto Networks PAN-OS® software on Panorama enables an attacker to cause a denial of service (DoS) condition. Repeated attempts to trigger this condition result in the Panorama entering maintenance mode.

Cloud NGFW, Prisma® Access, and standalone PAN-OS firewalls are not affected by this vulnerability.

Product Status:

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.2	< 12.2.4 on Panorama	>= 12.2.4 on Panorama
PAN-OS 12.1	< 12.1.4-h12 on Panorama < 12.1.7-h8 on Panorama < 12.1.10-h2 on Panorama	>= 12.1.4-h12 on Panorama >= 12.1.7-h8 on Panorama >= 12.1.10-h2 on Panorama
PAN-OS 11.2	< 11.2.4-h22 on Panorama < 11.2.7-h21 on Panorama < 11.2.10-h15 on Panorama < 11.2.13-h3 on Panorama < 11.2.15 on Panorama	>= 11.2.4-h22 on Panorama >= 11.2.7-h21 on Panorama >= 11.2.10-h15 on Panorama >= 11.2.13-h3 on Panorama >= 11.2.15 on Panorama
PAN-OS 11.1	< 11.1.4-h37 on Panorama < 11.1.6-h39 on Panorama < 11.1.7-h11 on Panorama < 11.1.10-h35 on Panorama < 11.1.13-h15 on Panorama < 11.1.16-h3 on Panorama	>= 11.1.4-h37 on Panorama >= 11.1.6-h39 on Panorama >= 11.1.7-h11 on Panorama >= 11.1.10-h35 on Panorama >= 11.1.13-h15 on Panorama >= 11.1.16-h3 on Panorama
Prisma Access	None	All

Solution:

Upgrade affected Panorama systems to the fixed versions identified in the Product Status table

CVE-2026-0314 GlobalProtect App: Local Denial of Service (DoS) on Windows CVSSv4.0 Base Score: 4.3

A type confusion vulnerability in Palo Alto Networks GlobalProtect™ app on Windows enables a local user with low privileges to cause a denial of service (DoS) condition.

The GlobalProtect™ app on Linux, macOS, iOS, Android, and Chrome OS is not affected by this vulnerability.

Product Status:

Versions	Affected	Unaffected
----------	----------	------------

GlobalProtect App	None on Linux None on macOS None on iOS None on Android None on Chrome OS	All on Linux All on macOS All on iOS All on Android All on Chrome OS
GlobalProtect App 6.3	< 6.3.3-h16 (6.3.3-1199) on Windows	>= 6.3.3-h16 (6.3.3-1199) on Windows
GlobalProtect App 6.2	< 6.2.8-h15 (6.2.8-1084) on Windows	>= 6.2.8-h15 (6.2.8-1084) on Windows
GlobalProtect App 6.0	< 6.0.15 on Windows	>= 6.0.15 on Windows

Solution:

Upgrade affected GlobalProtect App installations to the fixed versions identified in the Product Status table

CVE-2026-0312 Checkov by Prisma Cloud: Path Traversal Vulnerabilities CVSSv4.0 Base Score: 4.3

Path traversal vulnerabilities in Palo Alto Networks Checkov by Prisma® Cloud enable an unauthenticated local user to write files to arbitrary locations on the scanning filesystem.

Product Status:

Versions	Affected	Unaffected
Checkov by Prisma Cloud	< 3.3.25	>= 3.3.25

Solution:

Upgrade Checkov by Prisma Cloud to version **3.3.25 or later** as specified in the Product Status table.

CVE-2026-0317 PAN-OS: Denial of Service Vulnerability CVSSv4.0 Base Score: 1.2

A denial of service vulnerability in Palo Alto Networks PAN-OS software enables an authenticated user with a read-only administrator role to cause a denial of service (DoS) condition by sending a specially crafted API request.

The security risk posed by this issue is significantly minimized by restricting access to the management web interface to only trusted internal IP addresses.

Cloud NGFW, Panorama, and Prisma® Access are not affected by this vulnerability.

Product Status:

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.2	< 12.2.4	>= 12.2.4
PAN-OS 12.1	< 12.1.10-h2	>= 12.1.10-h2
PAN-OS 11.2	< 11.2.16	>= 11.2.16 (ETA: 10/15)
PAN-OS 11.1	< 11.1.16-h3	>= 11.1.16-h3
Prisma Access	None	All

Solution:

Upgrade affected PAN-OS systems to the fixed versions identified in the Product Status table.

CVE-2026-0316 PAN-OS: Stored Cross-Site Scripting (XSS) Vulnerability CVSSv4.0 Base Score: 1.1

A stored cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS® software enables a malicious authenticated administrator to store or execute a JavaScript payload using the web interface.

The security risk posed by this issue is minimized when the management interface is restricted to only trusted internal IP addresses.

This issue is applicable to PAN-OS® software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series).

Cloud NGFW and Prisma® Access are not affected by these vulnerabilities.

Product Status:

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.2	< 12.2.4	>= 12.2.4
PAN-OS 12.1	< 12.1.10-h2	>= 12.1.10-h2
PAN-OS 11.2	< 11.2.16	>= 11.2.16 (ETA: 10/15)
PAN-OS 11.1	< 11.1.16-h3	>= 11.1.16-h3

Prisma Access	None	All
---------------	------	-----

Solution:

Upgrade affected PAN-OS and Panorama systems to the fixed versions identified in the Product Status table

CVE-2026-0311 Checkov by Prisma Cloud: Server-Side Request Forgery
Vulnerability CVSSv4.0 Base Score: 1.1

A server-side request forgery vulnerability in Palo Alto Networks Checkov by Prisma® Cloud enables a local unauthenticated user to make unauthorized network requests from host to internal services.

Product Status:

Versions	Affected	Unaffected
Checkov by Prisma Cloud	< 3.2.533	>= 3.2.533

Solution:

Upgrade Checkov by Prisma Cloud to version 3.2.533 or later as specified in the Product Status table.

PAN-SA-2026-0013 Chromium: Monthly Vulnerability Update (October 2026)
CVSSv4.0 Base Score: 7.7

Palo Alto Networks incorporated the following Chromium security fixes into their products:

- [illegible]

Product Status:

Versions	Affected	Unaffected
Prisma Browser	< 152.8.5.83	>= 155.16.5.40

Solution:

Upgrade affected systems to the fixed versions identified in the Product Status table and apply vendor-recommended security updates.

Recommendations:

Smarttech247 team recommend the following actions to be taken:

- **Apply** appropriate patches or appropriate mitigations provided by Palo Alto to vulnerable systems immediately after appropriate testing.
- **Block** external access at the network boundary, unless external parties require service.
- **If global access isn't needed**, filter access to the affected computer at the network boundary. Restricting access to only trusted computers and networks might greatly reduce the likelihood of a successful exploit.
- **To reduce the impact of latent vulnerabilities**, always run non-administrative software as an unprivileged user with minimal access rights.

References:

- <https://security.paloaltonetworks.com/CVE-2026-0322>
- <https://security.paloaltonetworks.com/CVE-2026-0321>
- <https://security.paloaltonetworks.com/CVE-2026-0320>
- <https://security.paloaltonetworks.com/CVE-2026-0319>
- <https://security.paloaltonetworks.com/CVE-2026-0318>
- <https://security.paloaltonetworks.com/CVE-2026-0317>
- <https://security.paloaltonetworks.com/CVE-2026-0316>
- <https://security.paloaltonetworks.com/CVE-2026-0315>
- <https://security.paloaltonetworks.com/CVE-2026-0314>
- <https://security.paloaltonetworks.com/CVE-2026-0313>
- <https://security.paloaltonetworks.com/CVE-2026-0312>
- <https://security.paloaltonetworks.com/CVE-2026-0311>
- <https://security.paloaltonetworks.com/PAN-SA-2026-0013>

