Smarttech
YOUR 24/7 SECURITY PARTNER

Palo Alto Networks Security Advisories - 10th September 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	159
Authors	Mihaela Liliana Matei < mihaela.matei@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-10
Issue Date	2026-09-10

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, GlobalProtect App, Prisma Access Agent, Prisma Browser, Cortex XDR Broker VM, Checkov and related services. The disclosed issues buffer overflow, command injection, cross-site scripting (XSS), information disclosure, local privilege escalation, code execution, anti-tamper protection bypass, and endpoint DLP bypass vulnerabilities. The highest published severity in this release is CVSS 7.7 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-2026-0310 PAN-OS: Buffer Overflow Vulnerability via XML Processing
CVSSv4.0 Base Score: 7.2

A buffer overflow vulnerability in the XML processing functionality of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to the management web or dataplane interface to cause a denial of service (DoS) condition on VM-Series firewalls or execute arbitrary code with root privileges on the PA-Series firewalls.

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

Panorama is impacted by this vulnerability.

Affected Products:

Versions	Affected	Unaffected
Cloud NGFW	All on AWS* All on Azure*	None on AWS* None on Azure*
PAN-OS 12.2	< 12.2.3	>= 12.2.3
PAN-OS 12.1	< 12.1.4-h10 < 12.1.7-h5 < 12.1.10	>= 12.1.4-h10 >= 12.1.7-h5 >= 12.1.10
PAN-OS 11.2	< 11.2.4-h21 < 11.2.7-h20 < 11.2.10-h14 < 11.2.13-h2	>= 11.2.4-h21 >= 11.2.7-h20 >= 11.2.10-h14 >= 11.2.13-h2
PAN-OS 11.1	< 11.1.4-h36 < 11.1.6-h38 < 11.1.7-h10 < 11.1.10-h33 < 11.1.13-h12 < 11.1.16-h2	>= 11.1.4-h36 >= 11.1.6-h38 >= 11.1.7-h10 >= 11.1.10-h33 >= 11.1.13-h12 >= 11.1.16-h2
PAN-OS 10.2	< 10.2.7-h37 < 10.2.10-h40 < 10.2.13-h24 < 10.2.16-h10 < 10.2.18-h10	>= 10.2.7-h37 >= 10.2.10-h40 >= 10.2.13-h24 >= 10.2.16-h10 >= 10.2.18-h10
Prisma Access 12.1	< 12.1.7-h5*	>= 12.1.7-h5*
Prisma Access 11.2	< 11.2.7-h20*	>= 11.2.7-h20*
Prisma Access 10.2	< 10.2.10-h40*	>= 10.2.10-h40*

Solution:

Version	Minor Version	Suggested Solution
Cloud NGFW		Customers who prefer to upgrade can work with Palo Alto Networks support to schedule an on-demand software upgrade.
PAN-OS 12.2	12.2.0 through 12.2.2	Upgrade to 12.2.3 or later.
PAN-OS 12.1	12.1.8 through 12.1.9	Upgrade to 12.1.10 or later.
	12.1.5 through 12.1.7-h*	Upgrade to 12.1.7-h5 or 12.1.10 or later.
	12.1.2 through 12.1.4-h*	Upgrade to 12.1.4-h10 or 12.1.10 or later.
PAN-OS 11.2	11.2.11 through 11.2.13-h*	Upgrade to 11.2.13-h2 or later.
	11.2.8 through 11.2.10-h*	Upgrade to 11.2.10-h14 or later.
	11.2.5 through 11.2.7-h*	Upgrade to 11.2.7-h20 or later.
	11.2.0 through 11.2.4-h*	Upgrade to 11.2.4-h21 or later.
PAN-OS 11.1	11.1.14 through 11.1.16-h*	Upgrade to 11.1.16-h2 or later.
	11.1.11 through 11.1.13-h*	Upgrade to 11.1.13-h12 or later.
	11.1.8 through 11.1.10-h*	Upgrade to 11.1.10-h33 or later.
	11.1.7 through 11.1.7-h*	Upgrade to 11.1.7-h10 or later.
	11.1.5 through 11.1.6-h*	Upgrade to 11.1.6-h38 or later.
	11.1.0 through 11.1.4-h*	Upgrade to 11.1.4-h36 or later.
PAN-OS 10.2	10.2.17 through 10.2.18-h*	Upgrade to 10.2.18-h10 or later.
	10.2.14 through 10.2.16-h*	Upgrade to 10.2.16-h10 or later.
	10.2.11 through 10.2.13-h*	Upgrade to 10.2.13-h24 or later.

	10.2.8 through 10.2.10-h*	Upgrade to 10.2.10-h40 or later.
	10.2.0 through 10.2.7-h*	Upgrade to 10.2.7-h37 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access 12.1	12.1.2 through 12.1.*	Upgrade to 12.1.7-h5 or later.
Prisma Access 11.2	11.2.0 through 11.2*	Upgrade to 11.2.7-h20 or later.
Prisma Access 10.2	10.2.0 through 10.2.*	Upgrade to 10.2.10-h40 or later.

CVE-2026-0309 PAN-OS: Authenticated Command Injection in CLI with Luna HSM Configuration
CVSSv4.0 Base Score: 4

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 CLI and the device must be configured with a Luna Hardware Security Module (HSM).

The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators.

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

Affected Products:

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.2	< 12.2.3	>= 12.2.3
PAN-OS 12.1	< 12.1.4-h10 < 12.1.7-h5 < 12.1.10	>= 12.1.4-h10 >= 12.1.7-h5 >= 12.1.10
PAN-OS 11.2	< 11.2.4-h21 < 11.2.7-h20 < 11.2.10-h14 < 11.2.13-h2	>= 11.2.4-h21 >= 11.2.7-h20 >= 11.2.10-h14 >= 11.2.13-h2
PAN-OS 11.1	< 11.1.4-h36 < 11.1.6-h38 < 11.1.7-h10	>= 11.1.4-h36 >= 11.1.6-h38 >= 11.1.7-h10

	< 11.1.10-h33 **< 11.1.13-h12** **< 11.1.16-h2**	**>= 11.1.10-h33** **>= 11.1.13-h12** **>= 11.1.16-h2**
PAN-OS 10.2	**< 10.2.7-h37** **< 10.2.10-h40** **< 10.2.13-h24** **< 10.2.16-h10** **< 10.2.18-h10**	**>= 10.2.7-h37** **>= 10.2.10-h40** **>= 10.2.13-h24** **>= 10.2.16-h10** **>= 10.2.18-h10**
Prisma Access	**None**	**All**

Solution:

Version	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.2	12.2.0 through 12.2.2	Upgrade to 12.2.3 or later.
PAN-OS 12.1	12.1.8 through 12.1.9	Upgrade to 12.1.10 or later.
	12.1.5 through 12.1.7-h*	Upgrade to 12.1.7-h5 or 12.1.10 or later.
	12.1.2 through 12.1.4-h*	Upgrade to 12.1.4-h10 or 12.1.10 or later.
PAN-OS 11.2	11.2.11 through 11.2.13-h*	Upgrade to 11.2.13-h2 or later.
	11.2.8 through 11.2.10-h*	Upgrade to 11.2.10-h14 or later.
	11.2.5 through 11.2.7-h*	Upgrade to 11.2.7-h20 or later.
	11.2.0 through 11.2.4-h*	Upgrade to 11.2.4-h21 or later.
PAN-OS 11.1	11.1.14 through 11.1.16-h*	Upgrade or 11.1.16-h2 or later.
	11.1.11 through 11.1.13-h*	Upgrade to 11.1.13-h12 or later.
	11.1.8 through 11.1.10-h*	Upgrade to 11.1.10-h33 or later.
	11.1.7 through 11.1.7-h*	Upgrade to 11.1.7-h10 or later.
	11.1.5 through 11.1.6-h*	Upgrade to 11.1.6-h38 or later.
	11.1.0 through 11.1.4-h*	Upgrade to 11.1.4-h36 or later.
PAN-OS 10.2	10.2.17 through 10.2.18-h*	Upgrade to 10.2.18-h10 or later.
	10.2.14 through 10.2.16-h*	Upgrade to 10.2.16-h10 or later.
	10.2.11 through 10.2.13-h*	Upgrade to 10.2.13-h24 or later.
	10.2.8 through 10.2.10-h*	Upgrade to 10.2.10-h40 or later.
	10.2.0 through 10.2.7-h*	Upgrade to 10.2.7-h37 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.

Version	Minor Version	Suggested Solution
Prisma Access		No action needed.

CVE-2026-0308 PAN-OS: Stored Cross-Site Scripting (XSS) Vulnerability in the Web Interface
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.

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	None	All
PAN-OS 12.1	< 12.1.10	>= 12.1.10
PAN-OS 11.2	< 11.2.13-h2	>= 11.2.13-h2
PAN-OS 11.1	< 11.1.16-h2	>= 11.1.16-h2
Prisma Access	None	All

Solution:

Version	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.2		No action needed.
PAN-OS 12.1	12.1.2 through 12.1.9	Upgrade to 12.1.10 or later.
PAN-OS 11.2	11.2.0 through 11.2.13	Upgrade to 11.2.13-h2 or later.
PAN-OS 11.1	11.1.0 through 11.1.16	Upgrade to 11.1.16-h2 or later.
All older unsupported		Upgrade to a supported fixed version.

Version	Minor Version	Suggested Solution
PAN-OS versions		
Prisma Access		No action needed.

CVE-2026-0307 GlobalProtect App: Local Privilege Escalation Vulnerabilities
CVSSv4.0 Base Score: 5.9

Multiple local privilege escalation vulnerabilities in the Palo Alto Networks GlobalProtect™ app allows a local user to escalate their privileges to NT AUTHORITY\SYSTEM on Windows and root on macOS and Linux. This enables a non-administrative user to execute arbitrary commands with administrative privileges.

This GlobalProtect app on iOS, Android and ChromeOS is not impacted.

Affected Products:

Versions	Affected	Unaffected
GlobalProtect App	All on iOS All on Android All on ChromeOS	None on iOS None on Android None on ChromeOS
GlobalProtect App 6.3	< 6.3.3-h15 on Linux (ETA: 09/17) < 6.3.3-h15 on macOS (ETA: 09/28) < 6.3.3-h15 on Windows (ETA: 09/28)	>= 6.3.3-h15 on Linux (ETA: 09/17) >= 6.3.3-h15 on macOS (ETA: 09/28) >= 6.3.3-h15 on Windows (ETA: 09/28)
GlobalProtect App 6.2	< 6.2.8-h14 on macOS < 6.2.8-h14 on Windows	>= 6.2.8-h14 on macOS >= 6.2.8-h14 on Windows
GlobalProtect App 6.0	< 6.0.15 on Linux (ETA: 09/28) < 6.0.15 on macOS (ETA: 09/28) < 6.0.15 on Windows (ETA: 10/29)	>= 6.0.15 on Linux (ETA: 09/28) >= 6.0.15 on macOS (ETA: 09/28) >= 6.0.15 on Windows (ETA: 10/29)

Solution:

Version	Minor Version	Suggested Solution
GlobalProtect App 6.2/6.3 on Linux	6.2.0 through 6.3.3-h14	Upgrade to 6.3.3-h15 or later.
GlobalProtect App 6.0 on Linux	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.

Version	Minor Version	Suggested Solution
GlobalProtect App 6.3 on macOS	6.3.0 through 6.3.3-h14	Upgrade to 6.3.3-h15 or later.
GlobalProtect App 6.2 on macOS	6.2.0 through 6.2.8-h13	Upgrade to 6.2.8-h14 or later.
GlobalProtect App 6.0 on macOS	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.
GlobalProtect App 6.3 on Windows	6.3.0 through 6.3.3-h14	Upgrade to 6.3.3-h15 or later.
GlobalProtect App 6.2 on Windows	6.2.0 through 6.2.8-h13	Upgrade to 6.2.8-h14 or later.
GlobalProtect App 6.0 on Windows	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.
GlobalProtect App on iOS		No action needed.
GlobalProtect App on Android		No action needed.
GlobalProtect App on ChromeOS		No action needed.
PAN-OS 12.2	12.2.0 through 12.2.2	Upgrade to 12.2.3 or later.
PAN-OS 12.1	12.1.8 through 12.1.9	Upgrade to 12.1.10 or later.
	12.1.5 through 12.1.7-h*	Upgrade to 12.1.7-h5 or 12.1.10 or later.
	12.1.2 through 12.1.4-h*	Upgrade to 12.1.4-h10 or 12.1.10 or later.
PAN-OS 11.2	11.2.11 through 11.2.13-h*	Upgrade to 11.2.13-h2 or later.
	11.2.8 through 11.2.10-h*	Upgrade to 11.2.10-h14 or later.
	11.2.5 through 11.2.7-h*	Upgrade to 11.2.7-h20 or later.
	11.2.0 through 11.2.4-h*	Upgrade to 11.2.4-h21 or later.
PAN-OS 11.1	11.1.14 through 11.1.16-h*	Upgrade to 11.1.16 or 11.1.16-h2 or later.
	11.1.11 through 11.1.13-h*	Upgrade to 11.1.13-h12 or 11.1.16 or later.
	11.1.8 through 11.1.10-h*	Upgrade to 11.1.10-h33 or 11.1.16 or later.
	11.1.7 through 11.1.7-h*	Upgrade to 11.1.7-h10 or 11.1.16 or later.
	11.1.5 through 11.1.6-h*	Upgrade to 11.1.6-h38 or 11.1.16 or later.
	11.1.0 through 11.1.4-h*	Upgrade to 11.1.4-h36 or 11.1.16 or later.

Version	Minor Version	Suggested Solution
PAN-OS 10.2	10.2.17 through 10.2.18-h*	Upgrade to 10.2.18-h10 or later.
	10.2.14 through 10.2.16-h*	Upgrade to 10.2.16-h10 or 10.2.18 or later.
	10.2.11 through 10.2.13-h*	Upgrade to 10.2.13-h24 or 10.2.18 or later.
	10.2.8 through 10.2.10-h*	Upgrade to 10.2.10-h40 or 10.2.18 or later.
	10.2.0 through 10.2.7-h*	Upgrade to 10.2.7-h37 or 10.2.18 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access 12.1	12.1.2 through 12.1.*	Upgrade to 12.1.7-h5 or later.
Prisma Access 11.2	11.2.0 through 11.2*	Upgrade to 11.2.7-h20 or later.
Prisma Access 10.2	10.2.0 through 10.2.*	Upgrade to 10.2.10-h40 or later.

CVE-2026-0306 Prisma Access Agent: EndPoint DLP Bypass Vulnerability on Windows
CVSSv4.0 Base Score: 5.8

A vulnerability in the EndPoint Data Loss Prevention (DLP) enforcement of Palo Alto Networks Prisma® Access Agent enables a local user to bypass configured DLP policy enforcement controls and exfiltrate sensitive data.

This Prisma Access Agent on macOS, Linux, iOS, Android and Chrome OS is not affected.

Product Status:

Versions	Affected	Unaffected
Prisma Access Agent	None on Linux None on macOS None on iOS None on Android None on ChromeOS	All on Linux All on macOS All on iOS All on Android All on ChromeOS
Prisma Access Agent	< 26.2 on Windows	>= 26.2 on Windows

Solution:

Version	Minor Version	Suggested Solution
Prisma Access Agent on Windows	24.0 through 26.2	Upgrade to 26.2 or later.
Prisma Access Agent on Linux		No action needed.
Prisma Access Agent on macOS		No action needed.
Prisma Access Agent on iOS		No action needed.
Prisma Access Agent on Android		No action needed.
Prisma Access Agent on ChromeOS		No action needed.

CVE-2026-0305 Prisma Access Agent: Information Disclosure Vulnerability on Linux CVSSv4.0 Base Score: 4.3

An information disclosure vulnerability in the Palo Alto Networks Prisma® Access Agent on Linux enables a local user to access sensitive configuration data and credentials.

The Prisma Access Agent on macOS, Windows, iOS, Android and Chrome OS is not affected.

Product Status:

Versions	Affected	Unaffected
Prisma Access Agent	None on macOS None on Windows None on iOS None on Android None on ChromeOS	All on macOS All on Windows All on iOS All on Android All on ChromeOS
Prisma Access Agent 24.0	< 26.3 on Linux	>= 26.3 on Linux

Solution:

Version	Minor Version	Suggested Solution
Prisma Access Agent on Linux	25.7 through 26.2.2	Upgrade to 26.3 or later.
Prisma Access Agent on macOS		No action needed.
Prisma Access Agent on Windows		No action needed.
Prisma Access Agent on iOS		No action needed.
Prisma Access Agent on Android		No action needed.
Prisma Access Agent on ChromeOS		No action needed.

CVE-2026-0304 Cortex XDR Broker VM: Privilege Escalation Vulnerability
CVSSv4.0 Base Score: 4.8

A privilege escalation vulnerability in Palo Alto Networks Cortex XDR Broker VM enables an authenticated low privileged user with man-in-the-middle (MitM) access to execute code with root privileges on the Broker VM.

Product Status:

Versions	Affected	Unaffected
Cortex XDR Broker VM 20.0.96	< 32.0.52	>= 32.0.52

Solution:

This issue is fixed in Cortex XDR Broker VM 32.0.52, and all later Cortex XDR Broker VM versions.

- If automatic upgrades are enabled for Broker VM, then no action is required at this time.
- If automatic upgrades are not enabled for Broker VM, then we recommend that you do so to ensure that you always have the latest security patches installed in your software

CVE-2026-0303 Checkov by Prisma Cloud: Code Execution via Auto-Loaded Configuration File
CVSSv4.0 Base Score: 2.4

A code execution vulnerability in Palo Alto Networks Checkov by Prisma® Cloud can allow arbitrary code execution when Checkov scans a directory that contains an attacker-controlled configuration file.

Product Status:

Versions	Affected	Unaffected
Checkov by Prisma Cloud 3.2.0	< 3.2.532	>= 3.2.532

Solution:

Version	Minor Version	Suggested Solution
Checkov by Prisma Cloud 3.2	3.2.0 through 3.2.531	Upgrade to 3.2.532or later.

CVE-2026-0302 Checkov by Prisma Cloud: OS Command Injection Vulnerability
CVSSv4.0 Base Score: 1.1

An OS command injection vulnerability in Palo Alto Networks Checkov by Prisma® Cloud enables a local user to execute arbitrary commands in the processes running Checkov.

Product Status:

Versions	Affected	Unaffected
Checkov by Prisma Cloud 3.2.0	< 3.2.502	>= 3.2.502

Solution:

Version	Minor Version	Suggested Solution
Checkov by Prisma Cloud 3.2	3.2.0 through 3.2.501	Upgrade to 3.2.502 or later.

PAN-SA-2026-0012 Chromium: Monthly Vulnerability Update (September 2026)
CVSSv4.0 Base Score: 7.7

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

- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0404570826.html
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0826575033.html
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01815628406.html
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01193673229.html

CVE	Summary
CVE-2026-76020	Race condition in V8
CVE-2026-76022	Buffer overflow in Network
CVE-2026-76038	Type confusion in V8
CVE-2026-76046	Buffer overflow in ANGLE
CVE-2026-76047	Type confusion in V8
CVE-2026-79016	Observable discrepancy in SVG
CVE-2026-79032	Improper input validation in Network
CVE-2026-79118	Uninitialized resource in ANGLE
CVE-2026-79195	Use after free in Script
CVE-2026-79282	Use after free in ANGLE
CVE-2026-79286	Missing authorization in CustomTabs
CVE-2026-79290	Use after free in Aura
CVE-2026-79293	Information leak in Animation
CVE-2026-84348	Information leak in MediaCapture
CVE-2026-84350	Use after free in TabStrip
CVE-2026-84351	Buffer overflow in GPU

CVE-2026-84357	Improper input validation in Omnibox
CVE-2026-84358	Improper privilege management in Downloads
CVE-2026-84359	Information leak in Skia

Product Status:

Versions	Affected	Unaffected
Prisma Browser	< 151.26.5.170	>= 152.8.4.76

Solution:

CVE	Summary
CVE-2026-76038	151.26.5.170
CVE-2026-76046	151.26.5.170
CVE-2026-76047	151.26.5.170
CVE-2026-76020	151.26.6.174
CVE-2026-76022	151.26.6.174
CVE-2026-79016	152.8.3.65
CVE-2026-79032	152.8.3.65
CVE-2026-79118	152.8.3.65
CVE-2026-79195	152.8.3.65
CVE-2026-79282	152.8.3.65
CVE-2026-79286	152.8.3.65
CVE-2026-79290	152.8.3.65
CVE-2026-79293	152.8.3.65
CVE-2026-84348	152.8.4.76
CVE-2026-84350	152.8.4.76
CVE-2026-84351	152.8.4.76
CVE-2026-84357	152.8.4.76
CVE-2026-84358	152.8.4.76
CVE-2026-84359	152.8.4.76

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/PAN-SA-2026-0012
https://security.paloaltonetworks.com/CVE-2026-0302
https://security.paloaltonetworks.com/CVE-2026-0303
https://security.paloaltonetworks.com/CVE-2026-0304
https://security.paloaltonetworks.com/CVE-2026-0305
https://security.paloaltonetworks.com/CVE-2026-0306
https://security.paloaltonetworks.com/CVE-2026-0307
https://security.paloaltonetworks.com/CVE-2026-0308
https://security.paloaltonetworks.com/CVE-2026-0309
https://security.paloaltonetworks.com/CVE-2026-0310

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com