Smarttech
YOUR 24/7 SECURITY PARTNER

Palo Alto Networks Security Advisories - 12th February

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	24
Authors	Marian Matache <marian.matache@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-02-12
Issue Date	2026-02-12

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 vulnerabilities impacting its product portfolio, including several medium- to high-severity Chromium engine flaws in Prisma Browser that could allow remote code execution and UI spoofing via crafted web content. Additionally, a denial-of-service vulnerability in PAN-OS enables unauthenticated attackers to send malicious packets causing firewall reboots or forcing devices into maintenance mode. A separate low-severity certificate validation flaw affects PAN-OS deployments using Terminal Server Agents, potentially allowing connections with expired certificates. Patches addressing all issues have been released, and no active exploitation in the wild has been reported to date.

RISK:

Government:

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

Businesses:

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

TECHNICAL SUMMARY:

PAN-SA-2026-0002 Chromium: Monthly Vulnerability Update (February 2026)

CVSSv4.0 Base Score: 8.1

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

- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_28.html
- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/01/stable-channel-update-for-desktop_27.html

- https://chromereleases.googleblog.com/2026/01/stable-channel-update-for-desktop_20.html
- https://chromereleases.googleblog.com/2026/01/stable-channel-update-for-desktop_13.html

In addition to the above, Palo Alto has also fixed a vulnerability in the Prisma Access browser.

CVE	Summary
CVE-2026-0899	Out of bounds memory access in V8
CVE-2026-0900	Inappropriate implementation in V8
CVE-2026-0901	Inappropriate implementation in Blink
CVE-2026-0902	Inappropriate implementation in V8
CVE-2026-0903	Inappropriate implementation in Downloads
CVE-2026-0904	Incorrect security UI in Digital Credentials
CVE-2026-0905	Insufficient policy enforcement in Network
CVE-2026-0906	Incorrect security UI
CVE-2026-0907	Incorrect security UI in Split View
CVE-2026-0908	Use after free in ANGLE
CVE-2026-1504	Inappropriate implementation in Background Fetch API
CVE-2026-1861	Heap buffer overflow in libvpx
CVE-2026-1862	Type Confusion in V8

Affected Products:

Versions	Affected	Unaffected
Prisma Browser	< 144.27.7.133	>= 144.27.7.133

Solution:

CVE	Prisma Browser
CVE-2026-0899	144.6.10.59
CVE-2026-0900	144.6.10.59
CVE-2026-0901	144.6.10.59
CVE-2026-0902	144.6.10.59
CVE-2026-0903	144.6.10.59
CVE-2026-0904	144.6.10.59

CVE	Prisma Browser
CVE-2026-0905	144.6.10.59
CVE-2026-0906	144.6.10.59
CVE-2026-0907	144.6.10.59
CVE-2026-0908	144.6.10.59
CVE-2026-1504	144.23.6.110
CVE-2026-1861	144.27.7.133
CVE-2026-1862	144.27.7.133

CVE-2026-0229 PAN-OS: Denial of Service in Advanced DNS Security Feature

CVSSv4.0 Base Score: 6.6

A denial-of-service (DoS) vulnerability in the Advanced DNS Security (ADNS) feature of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker to initiate system reboots using a maliciously crafted packet. Repeated attempts to initiate a reboot causes the firewall to enter maintenance mode.

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

Affected Products:

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.4	>= 12.1.4
PAN-OS 11.2	< 11.2.10	>= 11.2.10
PAN-OS 11.1	None	All
PAN-OS 10.2	None	All
Prisma Access	None	All

Solution:

Version	Minor Version	Suggested Solution
Cloud NGFW All		No action needed.

Version	Minor Version	Suggested Solution
PAN-OS 12.1	12.1.2 through 12.1.3	Upgrade to 12.1.4 or later.
PAN-OS 11.2	11.2.0 through 11.2.9	Upgrade to 11.2.10 or later.
PAN-OS 11.1		No action needed.
PAN-OS 10.2		No action needed.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access All		No action needed.

CVE-2026-0228 PAN-OS: Improper Validation of Terminal Server Agent Certificate CVSSv4.0 Base Score: 1.3

An improper certificate validation vulnerability in PAN-OS allows users to connect Terminal Server Agents on Windows to PAN-OS using expired certificates even if the PAN-OS configuration would not normally permit them to do so.

Affected Products:

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	None	All
PAN-OS 11.2	< 11.2.8	>= 11.2.8
PAN-OS 11.1	< 11.1.11	>= 11.1.11
PAN-OS 10.2	< 10.2.17	>= 10.2.17
Prisma Access	< 10.2.10-h28 on PAN-OS < 11.2.7-h10 on PAN-OS	>= 10.2.10-h28 on PAN-OS >= 11.2.7-h10 on PAN-OS

Solution:

Version	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1		No action needed.

Version	Minor Version	Suggested Solution
PAN-OS 11.2	11.2.0 through 11.2.7	Upgrade to 11.2.8 or later.
PAN-OS 11.1	11.1.0 through 11.1.10	Upgrade to 11.1.11 or later.
PAN-OS 10.2	10.2.0 through 10.2.16	Upgrade to 10.2.17 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access 11.2 on PAN-OS	11.2.0 through 11.2.7	Upgrade to 11.2.7-h10 or later.
Prisma Access 10.2 on PAN-OS	10.2.0 through 10.2.10	Upgrade to 10.2.10-h28 or later.

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:

Palo Alto

- https://security.paloaltonetworks.com/PAN-SA-2026-0002
- https://security.paloaltonetworks.com/CVE-2026-0229
- https://security.paloaltonetworks.com/CVE-2026-0228

CVEs:

- https://nvd.nist.gov/vuln/detail/CVE-2026-0899
- https://nvd.nist.gov/vuln/detail/CVE-2026-0900
- https://nvd.nist.gov/vuln/detail/CVE-2026-0901
- https://nvd.nist.gov/vuln/detail/CVE-2026-0902
- https://nvd.nist.gov/vuln/detail/CVE-2026-0903
- https://nvd.nist.gov/vuln/detail/CVE-2026-0904
- https://nvd.nist.gov/vuln/detail/CVE-2026-0905
- https://nvd.nist.gov/vuln/detail/CVE-2026-0906
- https://nvd.nist.gov/vuln/detail/CVE-2026-0907
- https://nvd.nist.gov/vuln/detail/CVE-2026-0908
- https://nvd.nist.gov/vuln/detail/CCVE-2026-1504
- https://nvd.nist.gov/vuln/detail/CVE-2026-1861
- https://nvd.nist.gov/vuln/detail/CVE-2026-1862

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com