Smarttech
YOUR 24/7 SECURITY PARTNER

Palo Alto Networks Security Advisories - 9th July 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	110
Authors	Alex Ciuta <alexandru.ciuta@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-07-09
Issue Date	2026-07-08

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 affecting PAN-OS and related services, including buffer overflow flaws in the User-ID Terminal Server Agent that could allow unauthenticated attackers to trigger a denial-of-service condition or potentially execute arbitrary code, network traffic processing vulnerabilities that may force firewalls into maintenance mode through repeated DoS attacks, and a command injection flaw that enables authenticated administrators to execute arbitrary operating system commands as root. Palo Alto Networks has released fixes for all affected products and stated that it is not aware of any malicious exploitation of these vulnerabilities in the wild. Additionally, Prisma Browser received its monthly security update, incorporating the latest Chromium security fixes.

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-OS: Buffer Overflow Vulnerabilities in User-ID Terminal Server Agent

CVE: CVE-2026-0288
Score: 7.2
Description: Multiple buffer overflow vulnerabilities in the User-ID Terminal Server Agent (TSA) component of Palo Alto Networks PAN-OS software allow an unauthenticated attacker with network access to cause a denial of service (DoS) condition or potentially execute arbitrary code by sending specially crafted network traffic.

PAN-OS: Denial of Service Vulnerabilities in Network Traffic Processing

CVE: CVE-2026-0287
Score: 6.6
Description: Multiple 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 dataplane interface. Repeated attempts to trigger this condition result in the firewall entering maintenance mode.

PAN-OS: Authenticated Command Injection in CLI
CVE: CVE-2026-0286
Score: 6
Description: A command injection vulnerability in the management plane of Palo Alto Networks PAN-OS® software enables an authenticated administrator to execute arbitrary OS commands as root.

PAN-OS: Server-Side Request Forgery Vulnerability in Management Web Interface
CVE: CVE-2026-0285
Score: 4.7
Description: A server-side request forgery (SSRF) vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator with network access to the management web interface to make unauthorized requests from the firewall to internal services.

PAN-OS: XML Injection Vulnerability in Large Scale VPN (LSVPN)
CVE: CVE-2026-0284
Score: 4.7
Description: An XML injection vulnerability in the Large Scale VPN (LSVPN) functionality of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to inject malicious XML content, potentially leading to information disclosure or corruption of internal LSVPN satellite data.

PAN-OS: Authentication Bypass Vulnerability in Large Scale VPN (LSVPN)
CVE: CVE-2026-0283
Score: 4.5
Description: An authentication bypass vulnerability in Large Scale VPN (LSVPN) functionality of Palo Alto Networks PAN-OS software allows an attacker with network access to bypass security restrictions and establish an unauthorized site-to-site VPN connection.

PAN-OS: File Deletion Vulnerability in Management Web Interface
CVE: CVE-2026-0282
Score: 2.7
Description: A file deletion vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to the management web interface to delete files from a temporary directory.

PAN-OS: Information Disclosure Vulnerability in Management Web Interface
CVE: CVE-2026-0281
Score: 2.1
Description: An information disclosure vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to the management web interface to obtain web session tokens. This requires a legitimate user to first click on a malicious link provided by the attacker.

PAN-OS: IPv6 Firewall Policy Bypass

CVE: CVE-2026-0280
Score: 1.7
Description: An IPv6 packet processing vulnerability in the dataplane of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker to bypass firewall security policy enforcement, allowing network traffic that should be blocked to reach protected services.

PAN-OS: Multiple Cross-Site Scripting (XSS) Vulnerabilities

CVE: CVE-2026-0279
Score: 1.3
Description: Multiple cross site scripting vulnerabilities in the User-ID™ Authentication Portal (aka Captive Portal) service, GlobalProtect™ gateway/portal features and Clientless VPN of Palo Alto Networks PAN-OS® software enables a malicious unauthenticated user to store or execute malicious JavaScript payload.

Prisma Access Agent: Multiple DLP Policy Bypass Vulnerabilities on Windows

CVE: CVE-2026-0278
Score: 5.8
Description: Multiple protection mechanism failures in the Prisma Access Agent Data Loss Prevention (DLP) component for Windows allow a local user to bypass DLP policy enforcement controls.

Prisma Access Agent: Improper Certificate Validation on iOS

CVE: CVE-2026-0277
Score: 5.7
Description: An improper certificate validation vulnerability in the Prisma® Access Agent for iOS enables an attacker to perform a man-in-the-middle (MitM) attack to intercept VPN traffic.

Cortex XDR Broker VM: Privilege Escalation (PE) Vulnerability

CVE: CVE-2026-0276
Score: 1.1
Description: A privilege escalation vulnerability in Palo Alto Networks Cortex® XDR Broker VM enables a locally authenticated user to perform actions as the root user.

Chromium and Prisma Browser: Monthly Vulnerability Update (July 2026)

ID: PAN-SA-2026-0010
Score: 7.2
Description: Palo Alto Networks incorporated the following Chromium security fixes into our products:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_01245939337.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_01750511403.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_01962725236.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html

Affected Products:

PAN-OS: Buffer Overflow Vulnerabilities in User-ID Terminal Server Agent

Versions	Affected	Unaffected
Cloud NGFW	None on AWS None on Azure	All on AWS All on Azure unless you have been contacted by Palo Alto Networks
PAN-OS 12.1	< 12.1.4-h8 < 12.1.7-h2 < 12.1.8	>= 12.1.4-h8 >= 12.1.7-h2 >= 12.1.8
PAN-OS 11.2	< 11.2.4-h20 < 11.2.7-h18 < 11.2.10-h12 < 11.2.13	>= 11.2.4-h20 >= 11.2.7-h18 >= 11.2.10-h12 >= 11.2.13
PAN-OS 11.1	< 11.1.4-h35 < 11.1.6-h35 < 11.1.7-h8 < 11.1.10-h30 < 11.1.13-h9 < 11.1.16	>= 11.1.4-h35 >= 11.1.6-h35 >= 11.1.7-h8 >= 11.1.10-h30 >= 11.1.13-h9 >= 11.1.16
PAN-OS 10.2	< 10.2.7-h36 < 10.2.10-h39 < 10.2.13-h23 < 10.2.16-h9 < 10.2.18-h8	>= 10.2.7-h36 >= 10.2.10-h39 >= 10.2.13-h23 >= 10.2.16-h9 >= 10.2.18-h8
Prisma Access 11.2.0	< 11.2.7-h18*	>= 11.2.7-h18*
Prisma Access 10.2.0	< 10.2.10-h39*	>= 10.2.10-h39*

PAN-OS: Denial of Service Vulnerabilities in Network Traffic Processing

Versions	Affected	Unaffected
Cloud NGFW	All on AWS All on Azure	None on AWS None on Azure
PAN-OS 12.1	< 12.1.4-h8 < 12.1.7-h2 < 12.1.8	>= 12.1.4-h8 >= 12.1.7-h2 >= 12.1.8
PAN-OS 11.2	< 11.2.4-h20	>= 11.2.4-h20

	< 11.2.7-h18 < 11.2.10-h12 < 11.2.13	>= 11.2.7-h18 >= 11.2.10-h12 >= 11.2.13
PAN-OS 11.1	< 11.1.4-h35 < 11.1.6-h35 < 11.1.7-h8 < 11.1.10-h30 < 11.1.13-h9 < 11.1.16	>= 11.1.4-h35 >= 11.1.6-h35 >= 11.1.7-h8 >= 11.1.10-h30 >= 11.1.13-h9 >= 11.1.16
PAN-OS 10.2	< 10.2.7-h36 < 10.2.10-h39 < 10.2.13-h23 < 10.2.16-h9 < 10.2.18-h8	>= 10.2.7-h36 >= 10.2.10-h39 >= 10.2.13-h23 >= 10.2.16-h9 >= 10.2.18-h8
Prisma Access 11.2.0	< 11.2.7-h18*	>= 11.2.7-h18*
Prisma Access 10.2.0	< 10.2.10-h39*	>= 10.2.10-h39*

PAN-OS: Denial of Service Vulnerabilities in Network Traffic Processing

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.4-h8 < 12.1.7-h2 < 12.1.8	>= 12.1.4-h8 >= 12.1.7-h2 >= 12.1.8
PAN-OS 11.2	< 11.2.4-h20 < 11.2.7-h18 < 11.2.10-h11 < 11.2.13	>= 11.2.4-h20 >= 11.2.7-h18 >= 11.2.10-h11 >= 11.2.13
PAN-OS 11.1	< 11.1.4-h35 < 11.1.6-h35 < 11.1.7-h8 < 11.1.10-h30 < 11.1.13-h9 < 11.1.16	>= 11.1.4-h35 >= 11.1.6-h35 >= 11.1.7-h8 >= 11.1.10-h30 >= 11.1.13-h9 >= 11.1.16
PAN-OS 10.2	< 10.2.7-h36 < 10.2.10-h39 < 10.2.13-h23 < 10.2.16-h9 < 10.2.18-h8	>= 10.2.7-h36 >= 10.2.10-h39 >= 10.2.13-h23 >= 10.2.16-h9 >= 10.2.18-h8

Prisma Access	None	All

PAN-OS: Server-Side Request Forgery Vulnerability in Management Web Interface

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.4-h8 < 12.1.7-h2 < 12.1.8	>= 12.1.4-h8 >= 12.1.7-h2 >= 12.1.8
PAN-OS 11.2	< 11.2.4-h20 < 11.2.7-h18 < 11.2.10-h11 < 11.2.13	>= 11.2.4-h20 >= 11.2.7-h18 >= 11.2.10-h11 >= 11.2.13
PAN-OS 11.1	< 11.1.4-h35 < 11.1.6-h35 < 11.1.7-h8 < 11.1.10-h30 < 11.1.13-h9 < 11.1.16	>= 11.1.4-h35 >= 11.1.6-h35 >= 11.1.7-h8 >= 11.1.10-h30 >= 11.1.13-h9 >= 11.1.16
PAN-OS 10.2	< 10.2.7-h36 < 10.2.10-h39 < 10.2.13-h23 < 10.2.16-h9 < 10.2.18-h8	>= 10.2.7-h36 >= 10.2.10-h39 >= 10.2.13-h23 >= 10.2.16-h9 >= 10.2.18-h8
Prisma Access	None	All

PAN-OS: XML Injection Vulnerability in Large Scale VPN (LSVPN)

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.4-h8 < 12.1.7-h2 < 12.1.8	>= 12.1.4-h8 >= 12.1.7-h2 >= 12.1.8
PAN-OS 11.2	< 11.2.4-h20 < 11.2.7-h18 < 11.2.10-h11 < 11.2.13	>= 11.2.4-h20 >= 11.2.7-h18 >= 11.2.10-h11 >= 11.2.13
PAN-OS 11.1	< 11.1.4-h35	>= 11.1.4-h35

	< 11.1.6-h35 < 11.1.7-h8 < 11.1.10-h30 < 11.1.13-h9 < 11.1.16	>= 11.1.6-h35 >= 11.1.7-h8 >= 11.1.10-h30 >= 11.1.13-h9 >= 11.1.16
PAN-OS 10.2	< 10.2.7-h36 < 10.2.10-h39 < 10.2.13-h23 < 10.2.16-h9 < 10.2.18-h8	>= 10.2.7-h36 >= 10.2.10-h39 >= 10.2.13-h23 >= 10.2.16-h9 >= 10.2.18-h8
Prisma Access	None	All

PAN-OS: Authentication Bypass Vulnerability in Large Scale VPN (LSVPN)

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.4-h8 < 12.1.7-h2 < 12.1.8	>= 12.1.4-h8 >= 12.1.7-h2 >= 12.1.8
PAN-OS 11.2	< 11.2.4-h20 < 11.2.7-h18 < 11.2.10-h11 < 11.2.13	>= 11.2.4-h20 >= 11.2.7-h18 >= 11.2.10-h11 >= 11.2.13
PAN-OS 11.1	< 11.1.4-h35 < 11.1.6-h35 < 11.1.7-h8 < 11.1.10-h30 < 11.1.13-h9 < 11.1.16	>= 11.1.4-h35 >= 11.1.6-h35 >= 11.1.7-h8 >= 11.1.10-h30 >= 11.1.13-h9 >= 11.1.16
PAN-OS 10.2	< 10.2.7-h36 < 10.2.10-h39 < 10.2.13-h23 < 10.2.16-h9 < 10.2.18-h8	>= 10.2.7-h36 >= 10.2.10-h39 >= 10.2.13-h23 >= 10.2.16-h9 >= 10.2.18-h8
Prisma Access	None	All

PAN-OS: File Deletion Vulnerability in Management Web Interface

Versions	Affected	Unaffected

Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.8	>= 12.1.8
PAN-OS 11.2	< 11.2.13	>= 11.2.13
PAN-OS 11.1	< 11.1.16	>= 11.1.16
PAN-OS 10.2	All	None
Prisma Access	None	All

PAN-OS: Information Disclosure Vulnerability in Management Web Interface

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.8	>= 12.1.8
PAN-OS 11.2	< 11.2.13	>= 11.2.13
PAN-OS 11.1	< 11.1.16	>= 11.1.16
PAN-OS 10.2	All	None
Prisma Access	None	All

PAN-OS: IPv6 Firewall Policy Bypass

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.4-h8 < 12.1.7-h2 < 12.1.8	>= 12.1.4-h8 >= 12.1.7-h2 >= 12.1.8
PAN-OS 11.2	< 11.2.4-h20 < 11.2.7-h18 < 11.2.10-h11 < 11.2.13	>= 11.2.4-h20 >= 11.2.7-h18 >= 11.2.10-h11 >= 11.2.13
PAN-OS 11.1	< 11.1.4-h35 < 11.1.6-h35 < 11.1.7-h8	>= 11.1.4-h35 >= 11.1.6-h35 >= 11.1.7-h8

	< 11.1.10-h30 < 11.1.13-h9 < 11.1.16	>= 11.1.10-h30 >= 11.1.13-h9 >= 11.1.16
PAN-OS 10.2	< 10.2.7-h36 < 10.2.10-h39 < 10.2.13-h23 < 10.2.16-h9 < 10.2.18-h8	>= 10.2.7-h36 >= 10.2.10-h39 >= 10.2.13-h23 >= 10.2.16-h9 >= 10.2.18-h8
Panorama	None	All
Prisma Access 11.2.0	< 11.2.7-h18*	>= 11.2.7-h18*
Prisma Access 10.2.0	< 10.2.10-h39*	>= 10.2.10-h39*

PAN-OS: Multiple Cross-Site Scripting (XSS) Vulnerabilities

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.8	>= 12.1.8
PAN-OS 11.2	< 11.2.13	>= 11.2.13
PAN-OS 11.1	< 11.1.16	>= 11.1.16
PAN-OS 10.2	All	None
Prisma Access 12.1	< 12.1.8*	>= 12.1.8*
Prisma Access 11.1	All*	None*
Prisma Access 10.1	All*	None*

Prisma Access Agent: Multiple DLP Policy Bypass Vulnerabilities on Windows

Versions	Affected	Unaffected
Prisma Access Agent	None on macOS	All on macOS
Prisma Access Agent 0	< 26.2.1 on Windows	>= 26.2.1 on Windows

Prisma Access Agent: Improper Certificate Validation on iOS

Versions	Affected	Unaffected
Prisma Access Agent	None on Linux None on Windows None on macOS None on Android None on ChromeOS	All on Linux All on Windows All on macOS All on Android All on ChromeOS
Prisma Access Agent 0	< 26.2.1 on iOS	>= 26.2.1 on iOS

Cortex XDR Broker VM: Privilege Escalation (PE) Vulnerability

Versions	Affected	Unaffected
Cortex XDR Broker VM 20.0.96	< 31.0.58	>= 31.0.58

Solution:

PAN-OS: Buffer Overflow Vulnerabilities in User-ID Terminal Server Agent

Versions	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1	12.1.5 through 12.1.7-h* 12.1.2 through 12.1.4-h*	Upgrade to 12.1.7-h2 or 12.1.8 or later. Upgrade to 12.1.4-h8 or 12.1.8 or later.
PAN-OS 11.2	11.2.0 through 11.2.12 11.2.0 through 11.2.10-h* 11.2.0 through 11.2.7-h* 11.2.0 through 11.2.4-h*	Upgrade to 11.2.13 or later. Upgrade to 11.2.10-h12 or 11.2.13 or later. Upgrade to 11.2.7-h18 or 11.2.13 or later. Upgrade to 11.2.4-h20 or 11.2.13 or later.
PAN-OS 11.1	11.1.0 through 11.1.15 11.1.0 through 11.1.13-h* 11.1.0 through 11.1.10-h* 11.1.0 through 11.1.7-h* 11.1.0 through 11.1.6-h* 11.1.0 through 11.1.4-h*	Upgrade to 11.1.16 or later. Upgrade to 11.1.13-h9 or 11.1.16 or later. Upgrade to 11.1.10-h30 or 11.1.16 or later. Upgrade to 11.1.7-h8 or 11.1.16 or later. Upgrade to 11.1.6-h35 or 11.1.16 or later. Upgrade to 11.1.4-h35 or 11.1.16 or

		later.
PAN-OS 10.2	10.2.0 through 10.2.18-h* 10.2.0 through 10.2.16-h* 10.2.0 through 10.2.13-h* 10.2.0 through 10.2.10-h* 10.2.0 through 10.2.7-h*	Upgrade to 10.2.18-h8 or later. Upgrade to 10.2.16-h9 or later. Upgrade to 10.2.13-h23 or later. Upgrade to 10.2.10-h39 or later. Upgrade to 10.2.7-h36 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access 11.2	11.2.0 through 11.2.7	Upgrade to 11.2.7-h18 or later.*
Prisma Access 10.2	10.2.0 through 10.2.10	Upgrade to 10.2.10-h39 or later.*

PAN-OS: Denial of Service Vulnerabilities in Network Traffic Processing

Versions	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 12.1	12.1.5 through 12.1.7-h* 12.1.2 through 12.1.4-h*	Upgrade to 12.1.7-h2 or 12.1.8 or later. Upgrade to 12.1.4-h8 or 12.1.8 or later.
PAN-OS 11.2	11.2.0 through 11.2.12 11.2.0 through 11.2.10-h* 11.2.0 through 11.2.7-h* 11.2.0 through 11.2.4-h*	Upgrade to 11.2.13 or later. Upgrade to 11.2.10-h12 or 11.2.13 or later. Upgrade to 11.2.7-h18 or 11.2.13 or later. Upgrade to 11.2.4-h20 or 11.2.13 or later.
PAN-OS 11.1	11.1.0 through 11.1.15 11.1.0 through 11.1.13-h* 11.1.0 through 11.1.10-h* 11.1.0 through 11.1.7-h* 11.1.0 through 11.1.6-h* 11.1.0 through 11.1.4-h*	Upgrade to 11.1.16 or later. Upgrade to 11.1.13-h9 or 11.1.16 or later. Upgrade to 11.1.10-h30 or 11.1.16 or later. Upgrade to 11.1.7-h8 or 11.1.16 or later. Upgrade to 11.1.6-h35 or 11.1.16 or later. Upgrade to 11.1.4-h35 or 11.1.16 or later.
PAN-OS 10.2	10.2.0 through 10.2.18-h* 10.2.0 through 10.2.16-h* 10.2.0 through 10.2.13-h* 10.2.0 through 10.2.10-h*	Upgrade to 10.2.18-h8 or later. Upgrade to 10.2.16-h9 or later. Upgrade to 10.2.13-h23 or later. Upgrade to 10.2.10-h39 or later.

	10.2.0 through 10.2.7-h*	Upgrade to 10.2.7-h36 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access 11.2	11.2.0 through 11.2.7	Upgrade to 11.2.7-h18 or later.*
Prisma Access 10.2	10.2.0 through 10.2.10	Upgrade to 10.2.10-h39 or later.*

PAN-OS: Authenticated Command Injection in CLI

Versions	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1	12.1.5 through 12.1.7-h* 12.1.2 through 12.1.4-h*	Upgrade to 12.1.7-h2 or 12.1.8 or later. Upgrade to 12.1.4-h8 or 12.1.8 or later.
PAN-OS 11.2	11.2.11 through 11.2.12 11.2.8 through 11.2.10-h* 11.2.5 through 11.2.7-h* 11.2.0 through 11.2.4-h*	Upgrade to 11.2.13 or later. Upgrade to 11.2.10-h11 or 11.2.13 or later. Upgrade to 11.2.7-h18 or 11.2.13 or later. Upgrade to 11.2.4-h20 or 11.2.13 or later.
PAN-OS 11.1	11.1.14 through 11.1.15 11.1.11 through 11.1.13-h* 11.1.8 through 11.1.10-h* 11.1.7 through 11.1.7-h* 11.1.5 through 11.1.6-h* 11.1.0 through 11.1.4-h*	Upgrade to 11.1.16 or later. Upgrade to 11.1.13-h9 or 11.1.16 or later. Upgrade to 11.1.10-h30 or 11.1.16 or later. Upgrade to 11.1.7-h8 or 11.1.16 or later. Upgrade to 11.1.6-h35 or 11.1.16 or later. Upgrade to 11.1.4-h35 or 11.1.16 or later.
PAN-OS 10.2	10.2.17 through 10.2.18-h* 10.2.14 through 10.2.16-h* 10.2.11 through 10.2.13-h* 10.2.8 through 10.2.10-h* 10.2.0 through 10.2.7-h*	Upgrade to 10.2.18-h8 or later. Upgrade to 10.2.16-h9 or later. Upgrade to 10.2.13-h23 or later. Upgrade to 10.2.10-h39 or later. Upgrade to 10.2.7-h36 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access		No action needed.

PAN-OS: Server-Side Request Forgery Vulnerability in Management Web Interface

Versions	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1	12.1.5 through 12.1.7-h* 12.1.2 through 12.1.4-h*	Upgrade to 12.1.7-h2 or 12.1.8 or later. Upgrade to 12.1.4-h8 or 12.1.8 or later.
PAN-OS 11.2	11.2.11 through 11.2.12 11.2.8 through 11.2.10-h* 11.2.5 through 11.2.7-h* 11.2.0 through 11.2.4-h*	Upgrade to 11.2.13 or later. Upgrade to 11.2.10-h11 or 11.2.13 or later. Upgrade to 11.2.7-h18 or 11.2.13 or later. Upgrade to 11.2.4-h20 or 11.2.13 or later.
PAN-OS 11.1	11.1.14 through 11.1.15 11.1.11 through 11.1.13-h* 11.1.8 through 11.1.10-h* 11.1.7 through 11.1.7-h* 11.1.5 through 11.1.6-h* 11.1.0 through 11.1.4-h*	Upgrade to 11.1.16 or later. Upgrade to 11.1.13-h9 or 11.1.16 or later. Upgrade to 11.1.10-h30 or 11.1.16 or later. Upgrade to 11.1.7-h8 or 11.1.16 or later. Upgrade to 11.1.6-h35 or 11.1.16 or later. Upgrade to 11.1.4-h35 or 11.1.16 or later.
PAN-OS 10.2	10.2.17 through 10.2.18-h* 10.2.14 through 10.2.16-h* 10.2.11 through 10.2.13-h* 10.2.8 through 10.2.10-h* 10.2.0 through 10.2.7-h*	Upgrade to 10.2.18-h8 or later. Upgrade to 10.2.16-h9 or later. Upgrade to 10.2.13-h23 or later. Upgrade to 10.2.10-h39 or later. Upgrade to 10.2.7-h36 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access		No action needed.

PAN-OS: XML Injection Vulnerability in Large Scale VPN (LSVPN)

Versions	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1	12.1.5 through 12.1.7-h* 12.1.2 through 12.1.4-h*	Upgrade to 12.1.7-h2 or 12.1.8 or later. Upgrade to 12.1.4-h8 or 12.1.8 or later.

PAN-OS 11.2	11.2.11 through 11.2.12 11.2.8 through 11.2.10-h* 11.2.5 through 11.2.7-h* 11.2.0 through 11.2.4-h*	Upgrade to 11.2.13 or later. Upgrade to 11.2.10-h11 or 11.2.13 or later. Upgrade to 11.2.7-h18 or 11.2.13 or later. Upgrade to 11.2.4-h20 or 11.2.13 or later.
PAN-OS 11.1	11.1.14 through 11.1.15 11.1.11 through 11.1.13-h* 11.1.8 through 11.1.10-h* 11.1.7 through 11.1.7-h* 11.1.5 through 11.1.6-h* 11.1.0 through 11.1.4-h*	Upgrade to 11.1.16 or later. Upgrade to 11.1.13-h9 or 11.1.16 or later. Upgrade to 11.1.10-h30 or 11.1.16 or later. Upgrade to 11.1.7-h8 or 11.1.16 or later. Upgrade to 11.1.6-h35 or 11.1.16 or later. Upgrade to 11.1.4-h35 or 11.1.16 or later.
PAN-OS 10.2	10.2.17 through 10.2.18-h* 10.2.14 through 10.2.16-h* 10.2.11 through 10.2.13-h* 10.2.8 through 10.2.10-h* 10.2.0 through 10.2.7-h*	Upgrade to 10.2.18-h8 or later. Upgrade to 10.2.16-h9 or later. Upgrade to 10.2.13-h23 or later. Upgrade to 10.2.10-h39 or later. Upgrade to 10.2.7-h36 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access		No action needed.

PAN-OS: Authentication Bypass Vulnerability in Large Scale VPN (LSVPN)

Versions	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1	12.1.5 through 12.1.7-h* 12.1.2 through 12.1.4-h*	Upgrade to 12.1.7-h2 or 12.1.8 or later. Upgrade to 12.1.4-h8 or 12.1.8 or later.
PAN-OS 11.2	11.2.11 through 11.2.12 11.2.8 through 11.2.10-h* 11.2.5 through 11.2.7-h* 11.2.0 through 11.2.4-h*	Upgrade to 11.2.13 or later. Upgrade to 11.2.10-h11 or 11.2.13 or later. Upgrade to 11.2.7-h18 or 11.2.13 or later. Upgrade to 11.2.4-h20 or 11.2.13 or later.
PAN-OS 11.1	11.1.14 through 11.1.15 11.1.11 through 11.1.13-h* 11.1.8 through 11.1.10-h*	Upgrade to 11.1.16 or later. Upgrade to 11.1.13-h9 or 11.1.16 or later.

	11.1.7 through 11.1.7-h* 11.1.5 through 11.1.6-h* 11.1.0 through 11.1.4-h*	Upgrade to 11.1.10-h30 or 11.1.16 or later. Upgrade to 11.1.7-h8 or 11.1.16 or later. Upgrade to 11.1.6-h35 or 11.1.16 or later. Upgrade to 11.1.4-h35 or 11.1.16 or later.
PAN-OS 10.2	10.2.17 through 10.2.18-h* 10.2.14 through 10.2.16-h* 10.2.11 through 10.2.13-h* 10.2.8 through 10.2.10-h* 10.2.0 through 10.2.7-h*	Upgrade to 10.2.18-h8 or later. Upgrade to 10.2.16-h9 or later. Upgrade to 10.2.13-h23 or later. Upgrade to 10.2.10-h39 or later. Upgrade to 10.2.7-h36 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access		No action needed.

PAN-OS: File Deletion Vulnerability in Management Web Interface

Versions	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1	12.1.0 through 12.1.7-h*	Upgrade to 12.1.8 or later.
PAN-OS 11.2	11.2.0 through 11.2.12	Upgrade to 11.2.13 or later.
PAN-OS 11.1	11.1.0 through 11.1.15-h*	Upgrade to 11.1.16 or later.
PAN-OS 10.2	10.2.0 through 10.2*	Upgrade to 11.1.16 or 11.2.13 or 12.1.8 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access		No action needed.

PAN-OS: Information Disclosure Vulnerability in Management Web Interface

Versions	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1	12.1.0 through 12.1.7-h*	Upgrade to 12.1.8 or later.

PAN-OS 11.2	11.2.0 through 11.2.12	Upgrade to 11.2.13 or later.
PAN-OS 11.1	11.1.0 through 11.1.15-h*	Upgrade to 11.1.16 or later.
PAN-OS 10.2	10.2.0 through 10.2*	Upgrade to 11.1.16 or 11.2.13 or 12.1.8 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access		No action needed.

PAN-OS: IPv6 Firewall Policy Bypass

Versions	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1	12.1.5 through 12.1.7-h* 12.1.2 through 12.1.4-h*	Upgrade to 12.1.7-h2 or 12.1.8 or later. Upgrade to 12.1.4-h8 or 12.1.8 or later.
PAN-OS 11.2	11.2.11 through 11.2.12 11.2.8 through 11.2.10-h* 11.2.5 through 11.2.7-h* 11.2.0 through 11.2.4-h*	Upgrade to 11.2.13 or later. Upgrade to 11.2.10-h11 or 11.2.13 or later. Upgrade to 11.2.7-h18 or 11.2.13 or later. Upgrade to 11.2.4-h20 or 11.2.13 or later.
PAN-OS 11.1	11.1.14 through 11.1.15 11.1.11 through 11.1.13-h* 11.1.8 through 11.1.10-h* 11.1.7 through 11.1.7-h* 11.1.5 through 11.1.6-h* 11.1.0 through 11.1.4-h*	Upgrade to 11.1.16 or later. Upgrade to 11.1.13-h9 or 11.1.16 or later. Upgrade to 11.1.10-h30 or 11.1.16 or later. Upgrade to 11.1.7-h8 or 11.1.16 or later. Upgrade to 11.1.6-h35 or 11.1.16 or later. Upgrade to 11.1.4-h35 or 11.1.16 or later.
PAN-OS 10.2	10.2.17 through 10.2.18-h* 10.2.14 through 10.2.16-h* 10.2.11 through 10.2.13-h* 10.2.8 through 10.2.10-h* 10.2.0 through 10.2.7-h*	Upgrade to 10.2.18-h8 or later. Upgrade to 10.2.16-h9 or later. Upgrade to 10.2.13-h23 or later. Upgrade to 10.2.10-h39 or later. Upgrade to 10.2.7-h36 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.

Prisma Access 11.2	11.2.0 through 11.2.7	Upgrade to 11.2.7-h18 or later.*
Prisma Access 10.2	10.2.0 through 10.2.10	Upgrade to 10.2.10-h39 or later.*

PAN-OS: Multiple Cross-Site Scripting (XSS) Vulnerabilities

Versions	Minor Version	Suggested Solution
Cloud NGFW		No action needed.
PAN-OS 12.1	12.1.2 through 12.1.7-h*	Upgrade to 12.1.8 or later.
PAN-OS 11.2	11.2.0 through 11.2.12	Upgrade to 11.2.13 or later.
PAN-OS 11.1	11.1.0 through 11.1.15-h*	Upgrade to 11.1.16 or later.
PAN-OS 10.2	10.2.0 through 10.2*	Upgrade to 11.1.16, 11.2.13, 12.1.8 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access 12.2	12.1.2 through 12.1.7-h*	Upgrade to 12.1.8 or later.*
Prisma Access 11.2	11.2.0 through 11.2*	Upgrade to 12.1.8 or later.*
Prisma Access 10.2	10.2.0 through 10.2*	Upgrade to 12.1.8 or later.*

Prisma Access Agent: Multiple DLP Policy Bypass Vulnerabilities on Windows

Versions	Minor Version	Suggested Solution
Prisma Access Agent on Windows	24.0 through 26.2	Upgrade to 26.2.1 or later.
Prisma Access Agent on macOS		No action needed.

Prisma Access Agent: Improper Certificate Validation on iOS

Versions	Minor Version	Suggested Solution
Prisma Access	25.0 through 26.2	Upgrade to 26.2.1 or later.

Agent on iOS		
Prisma Access Agent on Linux		No action needed.
Prisma Access Agent on Windows		No action needed.
Prisma Access Agent on macOS		No action needed.
Prisma Access Agent on Android		No action needed.
Prisma Access Agent on ChromeOS		No action needed.

Cortex XDR Broker VM: Privilege Escalation (PE) Vulnerability

This issue is fixed in Cortex XDR Broker VM 31.0.58, 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.

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-2026-0288
https://security.paloaltonetworks.com/CVE-2026-0287
https://security.paloaltonetworks.com/CVE-2026-0286
https://security.paloaltonetworks.com/CVE-2026-0285
https://security.paloaltonetworks.com/CVE-2026-0284
https://security.paloaltonetworks.com/CVE-2026-0283
https://security.paloaltonetworks.com/CVE-2026-0282
https://security.paloaltonetworks.com/CVE-2026-0281
https://security.paloaltonetworks.com/CVE-2026-0280

https://security.paloaltonetworks.com/CVE-2026-0279
https://security.paloaltonetworks.com/CVE-2026-0278
https://security.paloaltonetworks.com/CVE-2026-0277
https://security.paloaltonetworks.com/CVE-2026-0276
https://security.paloaltonetworks.com/PAN-SA-2026-0010

CVEs:

CVE-2026-0288
CVE-2026-0287
CVE-2026-0286
CVE-2026-0285
CVE-2026-0284
CVE-2026-0283
CVE-2026-0282
CVE-2026-0281
CVE-2026-0280
CVE-2026-0279
CVE-2026-0278
CVE-2026-0277
CVE-2026-0276
PAN-SA-2026-0010


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com