Smarttech
YOUR 24/7 SECURITY PARTNER

Palo Alto Networks Security Advisories - 13th August 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	136
Authors	Maria Madalina Apetroaia < madalina.apetroaia@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-08-13
Issue Date	2026-08-13

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 and related services. The disclosed issues include information disclosure, local privilege escalation, buffer overflow, code execution, certificate validation bypass and anti-tamper protection bypass vulnerabilities. The highest published severity in this release is CVSS 7.2 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-2026-0301 PAN-OS: Information Disclosure Vulnerability in URL Filtering CVSSv4.0 Base Score: 1.7

An information disclosure vulnerability in PAN-OS URL Filtering may allow limited disclosure of information under specific conditions. The vulnerability affects multiple PAN-OS releases, Cloud NGFW deployments, and Prisma Access environments. Successful exploitation could expose information that may assist attackers in conducting further reconnaissance against affected environments. Palo Alto Networks has released fixes and remediated affected cloud-hosted services.

Affected Products:

Versions	Affected	Unaffected
Cloud NGFW	All on AWS* All on Azure*	None on AWS* None on Azure*
PAN-OS 12.1	None	All
PAN-OS 11.2	None	All
PAN-OS 11.1	< 11.1.16-h1 < 11.1.17	>= 11.1.16-h1 >= 11.1.17
PAN-OS 10.2	< 10.2.8	>= 10.2.8
Prisma Access 12.1	None	All

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 12.1	12.1.2 through 12.1.6-h*	No action needed.
PAN-OS 11.2	11.2.0 through 11.2.12	No action needed.
PAN-OS 11.1	11.1.0 through 11.1.16-h*	Upgrade to 11.1.16-h1 or 11.1.17 or later.
PAN-OS 10.2	10.2.0 through 10.2.*	Upgrade to 10.2.8 or 11.1.17 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access 12.1	12.1.2 through 12.1.*	No action needed.

CVE-2026-0299 GlobalProtect App: Local Privilege Escalation Vulnerabilities
CVSSv4.0 Base Score: 5.9

Multiple local privilege escalation vulnerabilities in the Palo Alto Networks GlobalProtect™ App enable a locally authenticated attacker to obtain elevated privileges on affected Windows, Linux, and macOS devices. Successful exploitation may allow attackers to gain administrative access, modify security settings, or further compromise affected endpoints. Android, iOS, and Chrome OS versions are not affected.

Affected Products:

Versions	Affected	Unaffected
GlobalProtect App	**None on iOS None on Android None on Chrome OS**	**All on iOS All on Android All on Chrome OS**
GlobalProtect App 6.3	**< 6.3.3-h15 on Linux < 6.3.3-h14 (6.3.3-1121) on macOS < 6.3.3-h14 (6.3.3-1121) on Windows**	**>= 6.3.3-h15 on Linux (ETA: 08/28) >= 6.3.3-h14 (6.3.3-1121) on macOS >= 6.3.3-h14 (6.3.3-1121) on Windows**
GlobalProtect App 6.2	**All on Linux < 6.2.8-h13 (6.2.8-1045) on macOS < 6.2.8-h13 (6.2.8-1045) on Windows**	**None on Linux >= 6.2.8-h13 (6.2.8-1045) on macOS >= 6.2.8-h13 (6.2.8-1045) on Windows**
GlobalProtect App 6.0	**< 6.0.15 on Linux < 6.0.15 on macOS < 6.0.15 on Windows**	**>= 6.0.15 on Linux (ETA: 08/31) >= 6.0.15 on macOS (ETA: 08/31) >= 6.0.15 on Windows (ETA: 08/31)**

Solution:

Version	Minor Version	Suggested Solution
GlobalProtect App 6.3/6.2 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.
GlobalProtect App 6.3 on macOS	6.3.0 through 6.3.3-h13	Upgrade to 6.3.3-h14 (6.3.3-1121) or later.
GlobalProtect App 6.3 on Windows	6.3.0 through 6.3.3-h13	Upgrade to 6.3.3-h14 (6.3.3-1121) or later.
GlobalProtect App 6.2 on macOS	6.2.0 through 6.2.8-h12	Upgrade to 6.2.8-h13 (6.2.8-1045) or later.
GlobalProtect App 6.2 on Windows	6.2.0 through 6.2.8-h12	Upgrade to 6.2.8-h13 (6.2.8-1045) or later.
GlobalProtect App 6.0 on macOS	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.
GlobalProtect App 6.0 on Windows	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.
GlobalProtect App on iOS		No action needed.

Version	Minor Version	Suggested Solution
GlobalProtect App on Android		No action needed.
GlobalProtect App on Chrome OS		No action needed.

CVE-2026-0298 GlobalProtect App: Code Execution Vulnerability in Windows Pre-Logon Access Provider (PLAP)
CVSSv4.0 Base Score: 5.2

A code execution vulnerability exists in the Windows Pre-Logon Access Provider (PLAP) component of the Palo Alto Networks GlobalProtect™ App. Successful exploitation could allow arbitrary code execution on vulnerable Windows systems.
Linux, macOS, Android, iOS, and Chrome OS versions are not affected.

Affected Products:

Versions	Affected	Unaffected
GlobalProtect App	None on Linux None on macOS None on Android None on Chrome OS None on iOS	All on Linux All on macOS All on Android All on Chrome OS All on iOS
GlobalProtect App 6.3	< 6.3.3-h14 (6.3.3-1121) on Windows	>= 6.3.3-h14 (6.3.3-1121) on Windows
GlobalProtect App 6.2	< 6.2.8-h13 (6.2.8-1045) on Windows	>= 6.2.8-h13 (6.2.8-1045) on Windows
GlobalProtect App 6.0	< 6.0.15 on Windows (ETA: 08/31)	>= 6.0.15 on Windows (ETA: 08/31)

Solution:

Version	Minor Version	Suggested Solution
GlobalProtect App 6.3 on Windows	6.3.0 through 6.3.3-h13	Upgrade to 6.3.3-h14 (6.3.3-1121) or later.
GlobalProtect App 6.2 on Windows	6.2.0 through 6.2.8-h12	Upgrade to 6.2.8-h13 (6.2.8-1045) or later.
GlobalProtect App 6.0 on Windows	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.
GlobalProtect App All on macOS		No action needed.
GlobalProtect App All on Linux		No action needed.

Version	Minor Version	Suggested Solution
GlobalProtect App All on iOS		No action needed.
GlobalProtect App All on Android		No action needed.
GlobalProtect App All on Chrome OS		No action needed.

CVE-2026-0297 GlobalProtect App: Buffer Overflow Vulnerability during UDP Tunnel Handshake
CVSSv4.0 Base Score: 5.2

A buffer overflow vulnerability exists in the Palo Alto Networks GlobalProtect™ app that enables a man-in-the-middle (MitM) attacker or a rogue gateway to disrupt system processes and potentially execute arbitrary code with elevated privileges (SYSTEM privileges on Windows, and root privileges on macOS and Linux).

Affected Products:

Versions	Affected	Unaffected
GlobalProtect App 6.3	< 6.3.3-h15 on Linux < 6.3.3-h14 (6.3.3-1121) on macOS < 6.3.3-h14 (6.3.3-1121) on Windows < 6.3.5 on iOS < 6.3.5 on Android < 6.3.5 on Chrome OS	>= 6.3.3-h15 on Linux (ETA: 08/28) >= 6.3.3-h14 (6.3.3-1121) on macOS >= 6.3.3-h14 (6.3.3-1121) on Windows >= 6.3.5 on iOS (ETA: 08/24) >= 6.3.5 on Android (ETA: 08/18) >= 6.3.5 on Chrome OS (ETA: 08/18)
GlobalProtect App 6.2	All on Linux < 6.2.8-h13 (6.2.8-1045) on macOS < 6.2.8-h13 (6.2.8-1045) on Windows	None on Linux >= 6.2.8-h13 (6.2.8-1045) on macOS >= 6.2.8-h13 (6.2.8-1045) on Windows
GlobalProtect App 6.0	< 6.0.15 on Linux < 6.0.15 on macOS < 6.0.15 on Windows < 6.0.15 on iOS < 6.0.15 on Android < 6.0.15 on Chrome OS	>= 6.0.15 on Linux (ETA: 08/31) >= 6.0.15 on macOS (ETA: 08/31) >= 6.0.15 on Windows (ETA: 08/31) >= 6.0.15 on iOS (ETA: 08/31) >= 6.0.15 on Android (ETA: 08/31)

		>= 6.0.15 on Chrome OS (ETA: 08/31)

Solution:

Version	Minor Version	Suggested Solution
GlobalProtect App 6.3/6.2 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.
GlobalProtect App 6.3 on macOS	6.3.0 through 6.3.3-h13	Upgrade to 6.3.3-h14 (6.3.3-1121) or later.
GlobalProtect App 6.2 on macOS	6.2.0 through 6.2.8-h12	Upgrade to 6.2.8-h13 (6.2.8-1045) 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-h13	Upgrade to 6.3.3-h14 (6.3.3-1121) or later.
GlobalProtect App 6.2 on Windows	6.2.0 through 6.2.8-h12	Upgrade to 6.2.8-h13 (6.2.8-1045) or later.
GlobalProtect App 6.0 on Windows	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.
GlobalProtect App 6.3/6.1 on iOS	6.1.0 through 6.3.4	Upgrade to 6.3.5 or later.
GlobalProtect App 6.0 on iOS	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.
GlobalProtect App 6.3/6.1 on Android	6.1.0 through 6.3.4	Upgrade to 6.3.5 or later.
GlobalProtect App 6.0 on Android	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.
GlobalProtect App 6.3/6.1 on ChromeOS	6.1.0 through 6.3.4	Upgrade to 6.3.5 or later.
GlobalProtect App 6.0 on ChromeOS	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.

CVE-2026-0296 GlobalProtect App: Improper Certificate Validation Bypass Vulnerability
CVSSv4.0 Base Score: 4.5

Improper certificate validation vulnerabilities in Palo Alto Networks GlobalProtect™ App enable an unauthenticated attacker with man-in-the-middle (MitM) access to intercept and modify application communications. VPN tunnel traffic is not impacted.

The GlobalProtect App on iOS, Android, and Chrome OS is not affected.

Product Status:

Versions	Affected	Unaffected
GlobalProtect App	None on iOS None on Android None on Chrome OS	All on iOS All on Android All on Chrome OS
GlobalProtect App 6.3	< 6.3.3-h15 on Linux < 6.3.3-h14 (6.3.3-1121) on macOS < 6.3.3-h14 (6.3.3-1121) on Windows	>= 6.3.3-h15 on Linux (ETA: 08/28) >= 6.3.3-h14 (6.3.3-1121) on macOS >= 6.3.3-h14 (6.3.3-1121) on Windows
GlobalProtect App 6.2	All on Linux < 6.2.8-h13 (6.2.8-1045) on macOS < 6.2.8-h13 (6.2.8-1045) on Windows	None on Linux >= 6.2.8-h13 (6.2.8-1045) on macOS >= 6.2.8-h13 (6.2.8-1045) on Windows
GlobalProtect App 6.0	< 6.0.15 on Linux < 6.0.15 on macOS < 6.0.15 on Windows	>= 6.0.15 on Linux (ETA: 08/31) >= 6.0.15 on macOS (ETA: 08/31) >= 6.0.15 on Windows (ETA: 08/31)

Solution:

Version	Minor Version	Suggested Solution
GlobalProtect App 6.3/6.2 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.
GlobalProtect App 6.3 on macOS	6.3.0 through 6.3.3-h13	Upgrade to 6.3.3-h14 (6.3.3-1121) or later.
GlobalProtect App 6.2 on macOS	6.2.0 through 6.2.8-h12	Upgrade to 6.2.8-h13 (6.2.8-1045) 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-h13	Upgrade to 6.3.3-h14 (6.3.3-1121) or later.
GlobalProtect App 6.2 on Windows	6.2.0 through 6.2.8-h12	Upgrade to 6.2.8-h13 (6.2.8-1045) or later.
GlobalProtect App 6.0 on Windows	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.

Version	Minor Version	Suggested Solution
GlobalProtect App on iOS		No action needed.
GlobalProtect App on Android		No action needed.
GlobalProtect App on Chrome OS		No action needed.

CVE-2026-0295 GlobalProtect App: Local Privilege Escalation via Race Condition on macOS
CVSSv4.0 Base Score: 4.1

A race condition in the Palo Alto Networks GlobalProtect™ client on macOS enables a locally authenticated low-privileged attacker to escalate their privileges to root.

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

Product Status:

Versions	Affected	Unaffected
GlobalProtect App	None on Linux None on Windows None on iOS None on Android None on Chrome OS	All on Linux All on Windows All on iOS All on Android All on Chrome OS
GlobalProtect App 6.3	< 6.3.3-h14 (6.3.3-1121) on macOS	>= 6.3.3-h14 (6.3.3-1121) on macOS
GlobalProtect App 6.2	< 6.2.8-h13 (6.2.8-1045) on macOS	>= 6.2.8-h13 (6.2.8-1045) on macOS
GlobalProtect App 6.0	< 6.0.15 on macOS	>= 6.0.15 on macOS (ETA: 08/31)

Solution:

Version	Minor Version	Suggested Solution
GlobalProtect App 6.3 on macOS	6.3.0 through 6.3.3-h13	Upgrade to 6.3.3-h14 (6.3.3-1121) or later.
GlobalProtect App 6.2 on macOS	6.2.0 through 6.2.8-h12	Upgrade to 6.2.8-h13 (6.2.8-1045) or later.
GlobalProtect App 6.0 on macOS	6.0.0 through 6.0.14	Upgrade to 6.0.15 or later.
GlobalProtect App on Linux		No action needed.

Version	Minor Version	Suggested Solution
GlobalProtect App on Windows		No action needed.
GlobalProtect App on iOS		No action needed.
GlobalProtect App on Android		No action needed.
GlobalProtect App on Chrome OS		No action needed.

CVE-2026-0294 Prisma Access Agent: Local Privilege Escalation
CVSSv4.0 Base Score: 6.0

A privilege escalation (PE) vulnerability in the Palo Alto Networks Prisma® Access Agent app on Windows and macOS devices enables a local user to execute code with elevated privileges.

The Prisma Access Agent on Linux, iOS, Android, and ChromeOS is not affected.

Product Status:

Versions	Affected	Unaffected
Prisma Access Agent	None on Linux None on iOS None on Android None on Chrome OS	All on Linux All on iOS All on Android All on Chrome OS
Prisma Access Agent	< 26.3 on Windows < 26.3 on macOS	>= 26.3 on Windows (ETA: 08/20) >= 26.3 on macOS (ETA: 08/20)

Solution:

Version	Minor Version	Suggested Solution
Prisma Access Agent on Windows	24.0 through 26.2.2	Upgrade to 26.3 or later.
Prisma Access Agent on macOS	24.0 through 26.2.2	Upgrade to 26.3 or later.
Prisma Access Agent on Linux		No action needed.
Prisma Access Agent on iOS		No action needed.
Prisma Access Agent on Android		No action needed.

CVE-2026-0293 Prisma Access Agent: Anti-Tamper Protection Bypass on Windows
CVSSv4.0 Base Score: 5.6

A vulnerability in Palo Alto Networks Prisma® Access Agent on Windows enables a local attacker with administrator privileges to bypass the anti-tamper protection, enabling unauthorized access to protected processes and files.

The Prisma Access Agent on Linux, macOS, 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 Chrome OS	All on Linux All on macOS All on iOS All on Android All on Chrome OS
Prisma Access Agent	< 26.3 on Windows	>= 26.3 on Windows (ETA: 08/20)

Solution:

Version	Minor Version	Suggested Solution
Prisma Access Agent on Windows	24.0 through 26.2.2	Upgrade to 26.3 or later.
Prisma Access Agent on macOS		No action needed.
Prisma Access Agent on Linux		No action needed.
Prisma Access Agent on iOS		No action needed.
Prisma Access Agent on Android		No action needed.
Prisma Access Agent on Chrome OS		No action needed.
All older unsupported versions		Upgrade to a supported fixed version

CVE-2026-0292 Prisma Access Agent: Local Security Inspection Bypass Vulnerability on Windows
CVSSv4.0 Base Score: 2.1

An authentication bypass vulnerability in the network driver of Palo Alto Networks Prisma® Access Agent on Windows enables a local administrator to bypass security inspection, subsequently allowing them to inject and intercept arbitrary network traffic.

The Prisma Access Agent on Linux, macOS, 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 Chrome OS	All on Linux All on macOS All on iOS All on Android All on Chrome OS
Prisma Access Agent	< 26.3 on Windows	>= 26.3 on Windows (ETA: 08/20)

Solution:

Version	Minor Version	Suggested Solution
Prisma Access Agent on Windows	24.0 through 26.2.2	Upgrade to 26.3 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 Chrome OS		No action needed.

CVE-2026-0291 Prisma Access Agent: Authenticated Limited File Deletion on Linux
CVSSv4.0 Base Score: 1.1

An improper link resolution before file access vulnerability exists in the Palo Alto Networks Prisma® Access Agent on Linux platforms. The vulnerability enables a local low-privileged user to delete system files in a limited scope and disable Prisma Access Agent.

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	All on macOS All on Windows All on iOS All on Android

	None on Chrome OS	All on Chrome OS
Prisma Access Agent	< 26.2.2 on Linux	>= 26.2.2 on Linux

Solution:

Version	Minor Version	Suggested Solution
Prisma Access Agent on Linux	25.7 through 26.2.1	Upgrade to 26.2.2 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 Chrome OS		No action needed.

PAN-SA-2026-0011 Chromium: Monthly Vulnerability Update (August 2026)
CVSSv4.0 Base Score: 7.2

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

- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_0887107924.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_01320465736.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_0256605430.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_049796704.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_0353146366.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_01162222768.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop.html

CVE	Summary
CVE-2026-4439	Out of bounds memory access in WebGL
CVE-2026-4440	Out of bounds read and write in WebGL
CVE-2026-4441	Use after free in Base
CVE-2026-4442	Heap buffer overflow in CSS
CVE-2026-4443	Heap buffer overflow in WebAudio
CVE-2026-4444	Stack buffer overflow in WebRTC
CVE-2026-4445	Use after free in WebRTC
CVE-2026-4446	Use after free in WebRTC
CVE-2026-4447	Inappropriate implementation in V8
CVE-2026-4448	Heap buffer overflow in ANGLE
CVE-2026-4449	Use after free in Blink
CVE-2026-4450	Out of bounds write in V8
CVE-2026-4451	Insufficient validation of untrusted input in Navigation
CVE-2026-4452	Integer overflow in ANGLE

CVE-2026-4453	Integer overflow in Dawn
CVE-2026-4454	Use after free in Network
CVE-2026-4455	Heap buffer overflow in PDFium
CVE-2026-4456	Use after free in Digital Credentials API
CVE-2026-4457	Type Confusion in V8
CVE-2026-4458	Use after free in Extensions
CVE-2026-4459	Out of bounds read and write in WebAudio
CVE-2026-4460	Out of bounds read in Skia
CVE-2026-4461	Inappropriate implementation in V8
CVE-2026-4462	Out of bounds read in Blink
CVE-2026-4463	Heap buffer overflow in WebRTC
CVE-2026-4464	Integer overflow in ANGLE
CVE-2026-4673	Heap buffer overflow in WebAudio
CVE-2026-4674	Out of bounds read in CSS
CVE-2026-4675	Heap buffer overflow in WebGL
CVE-2026-4676	Use after free in Dawn
CVE-2026-4677	Inappropriate implementation in WebAudio
CVE-2026-4678	Use after free in WebGPU
CVE-2026-4679	Integer overflow in Fonts
CVE-2026-4680	Use after free in FedCM
CVE-2026-5272	Heap buffer overflow in GPU
CVE-2026-5273	Use after free in CSS
CVE-2026-5274	Integer overflow in Codecs
CVE-2026-5275	Heap buffer overflow in ANGLE
CVE-2026-5276	Insufficient policy enforcement in WebUSB
CVE-2026-5277	Integer overflow in ANGLE
CVE-2026-5278	Use after free in Web MIDI
CVE-2026-5279	Object corruption in V8
CVE-2026-5280	Use after free in WebCodecs
CVE-2026-5281	Use after free in Dawn
CVE-2026-5282	Out of bounds read in WebCodecs
CVE-2026-5283	Inappropriate implementation in ANGLE
CVE-2026-5284	Use after free in Dawn
CVE-2026-5285	Use after free in WebGL
CVE-2026-5286	Use after free in Dawn
CVE-2026-5287	Use after free in PDF
CVE-2026-5288	Use after free in WebView
CVE-2026-5289	Use after free in Navigation
CVE-2026-5290	Use after free in Compositing
CVE-2026-5291	Inappropriate implementation in WebGL
CVE-2026-5292	Out of bounds read in WebCodecs
CVE-2026-5876	Side-channel information leakage in Navigation
CVE-2026-5881	Policy bypass in LocalNetworkAccess
CVE-2026-5884	Insufficient validation of untrusted input in Media
CVE-2026-5886	Out of bounds read in WebAudio
CVE-2026-5893	Race in V8
CVE-2026-5909	Integer overflow in Media
CVE-2026-5914	Type Confusion in CSS
CVE-2026-5919	Insufficient validation of untrusted input in WebSockets
CVE-2026-6305	Heap buffer overflow in PDFium
CVE-2026-6361	Heap buffer overflow in PDFium
CVE-2026-6921	Race in GPU
CVE-2026-7343	Use after free in Views
CVE-2026-7359	Use after free in ANGLE
CVE-2026-7361	Use after free in iOS
CVE-2026-7363	Use after free in Canvas
CVE-2026-7981	Out of bounds read in Codecs
CVE-2026-8018	Insufficient policy enforcement in DevTools
CVE-2026-8022	Inappropriate implementation in MHTML

CVE-2026-0237	Prisma Browser: Improperly Restricted Automation Bridge Allows Security Bypass
CVE-2026-0236	Prisma Browser: Code Injection Enables Security Controls Bypass
CVE-2026-0235	Prisma Browser: Access and Data Rule Bypass

Product Status:

Versions	Affected	Unaffected
Prisma Browser	< 148.18.4.217	>= 150.49.8.187

Solution:

CVE	Prisma Browser
CVE-2026-13774	150.41.2.115
CVE-2026-13775	150.41.2.115
CVE-2026-13776	150.41.2.115
CVE-2026-13777	150.41.2.115
CVE-2026-13778	150.41.2.115
CVE-2026-13779	150.41.2.115
CVE-2026-13780	150.41.2.115
CVE-2026-13781	150.41.2.115
CVE-2026-13782	150.41.2.115
CVE-2026-13783	150.41.2.115
CVE-2026-13784	150.41.2.115
CVE-2026-13785	150.41.2.115
CVE-2026-13786	150.41.2.115
CVE-2026-13787	150.41.2.115
CVE-2026-13788	150.41.2.115
CVE-2026-13789	150.41.2.115
CVE-2026-13790	150.41.2.115
CVE-2026-13791	150.41.2.115
CVE-2026-13792	150.41.2.115
CVE-2026-13793	150.41.2.115
CVE-2026-13794	150.41.2.115
CVE-2026-13795	150.41.2.115
CVE-2026-13796	150.41.2.115
CVE-2026-13797	150.41.2.115
CVE-2026-13798	150.41.2.115
CVE-2026-13799	150.41.2.115
CVE-2026-13800	150.41.2.115
CVE-2026-13801	150.41.2.115
CVE-2026-13802	150.41.2.115
CVE-2026-13803	150.41.2.115
CVE-2026-13804	150.41.2.115
CVE-2026-13805	150.41.2.115
CVE-2026-13806	150.41.2.115
CVE-2026-13807	150.41.2.115
CVE-2026-13808	150.41.2.115
CVE-2026-13809	150.41.2.115
CVE-2026-13810	150.41.2.115
CVE-2026-13811	150.41.2.115
CVE-2026-13812	150.41.2.115
CVE-2026-13813	150.41.2.115

CVE-2026-13814	150.41.2.115
CVE-2026-13815	150.41.2.115
CVE-2026-13816	150.41.2.115
CVE-2026-13817	150.41.2.115
CVE-2026-13818	150.41.2.115
CVE-2026-13819	150.41.2.115
CVE-2026-13820	150.41.2.115
CVE-2026-13821	150.41.2.115
CVE-2026-13822	150.41.2.115
CVE-2026-13823	150.41.2.115
CVE-2026-13824	150.41.2.115
CVE-2026-13825	150.41.2.115
CVE-2026-13826	150.41.2.115
CVE-2026-13827	150.41.2.115
CVE-2026-13828	150.41.2.115
CVE-2026-13829	150.41.2.115
CVE-2026-13830	150.41.2.115
CVE-2026-13831	150.41.2.115
CVE-2026-13832	150.41.2.115
CVE-2026-13833	150.41.2.115
CVE-2026-13834	150.41.2.115
CVE-2026-13835	150.41.2.115
CVE-2026-13836	150.41.2.115
CVE-2026-13837	150.41.2.115
CVE-2026-13838	150.41.2.115
CVE-2026-13839	150.41.2.115
CVE-2026-13840	150.41.2.115
CVE-2026-13841	150.41.2.115
CVE-2026-13842	150.41.2.115
CVE-2026-13843	150.41.2.115
CVE-2026-13844	150.41.2.115
CVE-2026-13845	150.41.2.115
CVE-2026-13846	150.41.2.115
CVE-2026-13847	150.41.2.115
CVE-2026-13848	150.41.2.115
CVE-2026-13849	150.41.2.115
CVE-2026-13850	150.41.2.115
CVE-2026-13851	150.41.2.115
CVE-2026-13852	150.41.2.115
CVE-2026-13853	150.41.2.115
CVE-2026-13854	150.41.2.115
CVE-2026-13855	150.41.2.115
CVE-2026-13856	150.41.2.115
CVE-2026-13857	150.41.2.115
CVE-2026-13858	150.41.2.115
CVE-2026-13859	150.41.2.115
CVE-2026-13860	150.41.2.115
CVE-2026-13861	150.41.2.115
CVE-2026-13862	150.41.2.115
CVE-2026-13863	150.41.2.115
CVE-2026-13864	150.41.2.115
CVE-2026-13865	150.41.2.115
CVE-2026-13866	150.41.2.115
CVE-2026-13867	150.41.2.115
CVE-2026-13868	150.41.2.115
CVE-2026-13869	150.41.2.115
CVE-2026-13870	150.41.2.115
CVE-2026-13871	150.41.2.115
CVE-2026-13872	150.41.2.115

CVE-2026-13873	150.41.2.115
CVE-2026-13874	150.41.2.115
CVE-2026-13875	150.41.2.115
CVE-2026-13876	150.41.2.115
CVE-2026-13877	150.41.2.115
CVE-2026-13878	150.41.2.115
CVE-2026-13879	150.41.2.115
CVE-2026-13880	150.41.2.115
CVE-2026-13881	150.41.2.115
CVE-2026-13882	150.41.2.115
CVE-2026-13883	150.41.2.115
CVE-2026-13884	150.41.2.115
CVE-2026-13885	150.41.2.115
CVE-2026-13886	150.41.2.115
CVE-2026-13887	150.41.2.115
CVE-2026-13888	150.41.2.115
CVE-2026-13889	150.41.2.115
CVE-2026-13890	150.41.2.115
CVE-2026-13891	150.41.2.115
CVE-2026-13892	150.41.2.115
CVE-2026-13893	150.41.2.115
CVE-2026-13894	150.41.2.115
CVE-2026-13895	150.41.2.115
CVE-2026-13896	150.41.2.115
CVE-2026-13897	150.41.2.115
CVE-2026-13898	150.41.2.115
CVE-2026-13899	150.41.2.115
CVE-2026-13900	150.41.2.115
CVE-2026-13901	150.41.2.115
CVE-2026-13902	150.41.2.115
CVE-2026-13903	150.41.2.115
CVE-2026-13904	150.41.2.115
CVE-2026-13905	150.41.2.115
CVE-2026-13906	150.41.2.115
CVE-2026-13907	150.41.2.115
CVE-2026-13908	150.41.2.115
CVE-2026-13909	150.41.2.115
CVE-2026-13910	150.41.2.115
CVE-2026-13911	150.41.2.115
CVE-2026-13912	150.41.2.115
CVE-2026-13913	150.41.2.115
CVE-2026-13914	150.41.2.115
CVE-2026-13915	150.41.2.115
CVE-2026-13916	150.41.2.115
CVE-2026-13917	150.41.2.115
CVE-2026-13918	150.41.2.115
CVE-2026-13919	150.41.2.115
CVE-2026-13920	150.41.2.115
CVE-2026-13921	150.41.2.115
CVE-2026-13922	150.41.2.115
CVE-2026-13923	150.41.2.115
CVE-2026-13924	150.41.2.115
CVE-2026-13925	150.41.2.115
CVE-2026-13926	150.41.2.115
CVE-2026-13927	150.41.2.115
CVE-2026-13928	150.41.2.115
CVE-2026-13929	150.41.2.115
CVE-2026-13930	150.41.2.115
CVE-2026-13931	150.41.2.115

CVE-2026-13932	150.41.2.115
CVE-2026-13933	150.41.2.115
CVE-2026-13934	150.41.2.115
CVE-2026-13935	150.41.2.115
CVE-2026-13936	150.41.2.115
CVE-2026-13937	150.41.2.115
CVE-2026-13938	150.41.2.115
CVE-2026-13939	150.41.2.115
CVE-2026-13940	150.41.2.115
CVE-2026-13941	150.41.2.115
CVE-2026-13942	150.41.2.115
CVE-2026-13943	150.41.2.115
CVE-2026-13944	150.41.2.115
CVE-2026-13945	150.41.2.115
CVE-2026-13946	150.41.2.115
CVE-2026-13947	150.41.2.115
CVE-2026-13948	150.41.2.115
CVE-2026-13949	150.41.2.115
CVE-2026-13950	150.41.2.115
CVE-2026-13951	150.41.2.115
CVE-2026-13952	150.41.2.115
CVE-2026-13953	150.41.2.115
CVE-2026-13954	150.41.2.115
CVE-2026-13955	150.41.2.115
CVE-2026-13956	150.41.2.115
CVE-2026-13957	150.41.2.115
CVE-2026-13958	150.41.2.115
CVE-2026-13959	150.41.2.115
CVE-2026-13960	150.41.2.115
CVE-2026-13961	150.41.2.115
CVE-2026-13962	150.41.2.115
CVE-2026-13963	150.41.2.115
CVE-2026-13964	150.41.2.115
CVE-2026-13965	150.41.2.115
CVE-2026-13966	150.41.2.115
CVE-2026-13967	150.41.2.115
CVE-2026-13968	150.41.2.115
CVE-2026-13969	150.41.2.115
CVE-2026-13970	150.41.2.115
CVE-2026-13971	150.41.2.115
CVE-2026-13972	150.41.2.115
CVE-2026-13973	150.41.2.115
CVE-2026-13974	150.41.2.115
CVE-2026-13975	150.41.2.115
CVE-2026-13976	150.41.2.115
CVE-2026-13977	150.41.2.115
CVE-2026-13978	150.41.2.115
CVE-2026-13979	150.41.2.115
CVE-2026-13980	150.41.2.115
CVE-2026-13981	150.41.2.115
CVE-2026-13982	150.41.2.115
CVE-2026-13983	150.41.2.115
CVE-2026-13984	150.41.2.115
CVE-2026-13985	150.41.2.115
CVE-2026-13986	150.41.2.115
CVE-2026-13987	150.41.2.115
CVE-2026-13988	150.41.2.115
CVE-2026-13989	150.41.2.115
CVE-2026-13990	150.41.2.115

CVE-2026-13991	150.41.2.115
CVE-2026-13992	150.41.2.115
CVE-2026-13993	150.41.2.115
CVE-2026-13994	150.41.2.115
CVE-2026-13995	150.41.2.115
CVE-2026-13996	150.41.2.115
CVE-2026-13997	150.41.2.115
CVE-2026-13998	150.41.2.115
CVE-2026-13999	150.41.2.115
CVE-2026-14000	150.41.2.115
CVE-2026-14001	150.41.2.115
CVE-2026-14002	150.41.2.115
CVE-2026-14003	150.41.2.115
CVE-2026-14004	150.41.2.115
CVE-2026-14005	150.41.2.115
CVE-2026-14006	150.41.2.115
CVE-2026-14007	150.41.2.115
CVE-2026-14008	150.41.2.115
CVE-2026-14009	150.41.2.115
CVE-2026-14010	150.41.2.115
CVE-2026-14011	150.41.2.115
CVE-2026-14012	150.41.2.115
CVE-2026-14013	150.41.2.115
CVE-2026-14014	150.41.2.115
CVE-2026-14015	150.41.2.115
CVE-2026-14016	150.41.2.115
CVE-2026-14017	150.41.2.115
CVE-2026-14018	150.41.2.115
CVE-2026-14019	150.41.2.115
CVE-2026-14020	150.41.2.115
CVE-2026-14021	150.41.2.115
CVE-2026-14022	150.41.2.115
CVE-2026-14023	150.41.2.115
CVE-2026-14024	150.41.2.115
CVE-2026-14025	150.41.2.115
CVE-2026-14026	150.41.2.115
CVE-2026-14027	150.41.2.115
CVE-2026-14028	150.41.2.115
CVE-2026-14030	150.41.2.115
CVE-2026-14031	150.41.2.115
CVE-2026-14032	150.41.2.115
CVE-2026-14033	150.41.2.115
CVE-2026-14034	150.41.2.115
CVE-2026-14035	150.41.2.115
CVE-2026-14036	150.41.2.115
CVE-2026-14037	150.41.2.115
CVE-2026-14038	150.41.2.115
CVE-2026-14039	150.41.2.115
CVE-2026-14040	150.41.2.115
CVE-2026-14041	150.41.2.115
CVE-2026-14042	150.41.2.115
CVE-2026-14043	150.41.2.115
CVE-2026-14044	150.41.2.115
CVE-2026-14045	150.41.2.115
CVE-2026-14046	150.41.2.115
CVE-2026-14047	150.41.2.115
CVE-2026-14048	150.41.2.115
CVE-2026-14049	150.41.2.115
CVE-2026-14050	150.41.2.115

CVE-2026-14051	150.41.2.115
CVE-2026-14052	150.41.2.115
CVE-2026-14053	150.41.2.115
CVE-2026-14054	150.41.2.115
CVE-2026-14055	150.41.2.115
CVE-2026-14056	150.41.2.115
CVE-2026-14057	150.41.2.115
CVE-2026-14058	150.41.2.115
CVE-2026-14059	150.41.2.115
CVE-2026-14060	150.41.2.115
CVE-2026-14061	150.41.2.115
CVE-2026-14062	150.41.2.115
CVE-2026-14063	150.41.2.115
CVE-2026-14064	150.41.2.115
CVE-2026-14065	150.41.2.115
CVE-2026-14066	150.41.2.115
CVE-2026-14067	150.41.2.115
CVE-2026-14068	150.41.2.115
CVE-2026-14069	150.41.2.115
CVE-2026-14070	150.41.2.115
CVE-2026-14071	150.41.2.115
CVE-2026-14072	150.41.2.115
CVE-2026-14073	150.41.2.115
CVE-2026-14074	150.41.2.115
CVE-2026-14075	150.41.2.115
CVE-2026-14076	150.41.2.115
CVE-2026-14077	150.41.2.115
CVE-2026-14078	150.41.2.115
CVE-2026-14079	150.41.2.115
CVE-2026-14080	150.41.2.115
CVE-2026-14081	150.41.2.115
CVE-2026-14082	150.41.2.115
CVE-2026-14083	150.41.2.115
CVE-2026-14084	150.41.2.115
CVE-2026-14085	150.41.2.115
CVE-2026-14086	150.41.2.115
CVE-2026-14087	150.41.2.115
CVE-2026-14088	150.41.2.115
CVE-2026-14089	150.41.2.115
CVE-2026-14090	150.41.2.115
CVE-2026-14091	150.41.2.115
CVE-2026-14092	150.41.2.115
CVE-2026-14093	150.41.2.115
CVE-2026-14094	150.41.2.115
CVE-2026-14095	150.41.2.115
CVE-2026-14096	150.41.2.115
CVE-2026-14097	150.41.2.115
CVE-2026-14098	150.41.2.115
CVE-2026-14099	150.41.2.115
CVE-2026-14100	150.41.2.115
CVE-2026-14101	150.41.2.115
CVE-2026-14102	150.41.2.115
CVE-2026-14103	150.41.2.115
CVE-2026-14104	150.41.2.115
CVE-2026-14105	150.41.2.115
CVE-2026-14106	150.41.2.115
CVE-2026-14107	150.41.2.115
CVE-2026-14108	150.41.2.115
CVE-2026-14109	150.41.2.115

CVE-2026-14110	150.41.2.115
CVE-2026-14111	150.41.2.115
CVE-2026-14112	150.41.2.115
CVE-2026-14113	150.41.2.115
CVE-2026-14114	150.41.2.115
CVE-2026-14115	150.41.2.115
CVE-2026-14116	150.41.2.115
CVE-2026-14117	150.41.2.115
CVE-2026-14118	150.41.2.115
CVE-2026-14119	150.41.2.115
CVE-2026-14120	150.41.2.115
CVE-2026-14121	150.41.2.115
CVE-2026-14122	150.41.2.115
CVE-2026-14123	150.41.2.115
CVE-2026-14124	150.41.2.115
CVE-2026-14125	150.41.2.115
CVE-2026-14126	150.41.2.115
CVE-2026-14127	150.41.2.115
CVE-2026-14128	150.41.2.115
CVE-2026-14129	150.41.2.115
CVE-2026-14130	150.41.2.115
CVE-2026-14131	150.41.2.115
CVE-2026-14132	150.41.2.115
CVE-2026-14133	150.41.2.115
CVE-2026-14134	150.41.2.115
CVE-2026-14135	150.41.2.115
CVE-2026-14136	150.41.2.115
CVE-2026-14137	150.41.2.115
CVE-2026-14138	150.41.2.115
CVE-2026-14139	150.41.2.115
CVE-2026-14140	150.41.2.115
CVE-2026-14141	150.41.2.115
CVE-2026-14142	150.41.2.115
CVE-2026-14143	150.41.2.115
CVE-2026-14144	150.41.2.115
CVE-2026-14145	150.41.2.115
CVE-2026-14146	150.41.2.115
CVE-2026-14147	150.41.2.115
CVE-2026-14148	150.41.2.115
CVE-2026-14149	150.41.2.115
CVE-2026-14150	150.41.2.115
CVE-2026-14151	150.41.2.115
CVE-2026-14152	150.41.2.115
CVE-2026-14153	150.41.2.115
CVE-2026-14154	150.41.2.115
CVE-2026-14155	150.41.2.115
CVE-2026-14156	150.41.2.115
CVE-2026-15107	150.41.2.115
CVE-2026-15108	150.41.2.115
CVE-2026-15109	150.41.2.115
CVE-2026-15110	150.41.2.115
CVE-2026-15111	150.41.2.115
CVE-2026-15112	150.41.2.115
CVE-2026-15113	150.41.2.115
CVE-2026-15114	150.41.2.115
CVE-2026-15115	150.41.2.115
CVE-2026-15116	150.41.2.115
CVE-2026-15117	150.41.2.115
CVE-2026-15118	150.41.2.115

CVE-2026-15119	150.41.2.115
CVE-2026-15120	150.41.2.115
CVE-2026-15121	150.41.2.115
CVE-2026-15122	150.41.2.115
CVE-2026-15123	150.41.2.115
CVE-2026-15124	150.41.2.115
CVE-2026-15125	150.41.2.115
CVE-2026-15126	150.41.2.115
CVE-2026-15127	150.41.2.115
CVE-2026-15128	150.41.2.115
CVE-2026-15129	150.41.2.115
CVE-2026-15130	150.41.2.115
CVE-2026-15131	150.41.2.115
CVE-2026-15132	150.41.2.115
CVE-2026-15133	150.41.2.115
CVE-2026-15764	150.49.4.125
CVE-2026-15765	150.49.4.125
CVE-2026-15766	150.49.4.125
CVE-2026-15767	150.49.4.125
CVE-2026-15768	150.49.4.125
CVE-2026-15769	150.49.4.125
CVE-2026-15770	150.49.4.125
CVE-2026-15771	150.49.4.125
CVE-2026-15772	150.49.4.125
CVE-2026-15773	150.49.4.125
CVE-2026-15774	150.49.4.125
CVE-2026-15775	150.49.4.125
CVE-2026-15776	150.49.4.125
CVE-2026-15777	150.49.4.125
CVE-2026-15778	150.49.4.125
CVE-2026-15899	150.49.6.129
CVE-2026-15900	150.49.6.129
CVE-2026-15901	150.49.6.129
CVE-2026-15902	150.49.6.129
CVE-2026-15903	150.49.6.129
CVE-2026-15904	150.49.6.129
CVE-2026-15905	150.49.6.129
CVE-2026-16413	150.49.7.182
CVE-2026-16414	150.49.7.182
CVE-2026-16415	150.49.7.182
CVE-2026-16416	150.49.7.182
CVE-2026-16417	150.49.7.182
CVE-2026-16418	150.49.7.182
CVE-2026-16419	150.49.7.182
CVE-2026-16420	150.49.7.182
CVE-2026-16421	150.49.7.182
CVE-2026-16422	150.49.7.182
CVE-2026-16423	150.49.7.182
CVE-2026-16424	150.49.7.182
CVE-2026-16804	150.49.8.187
CVE-2026-16805	150.49.8.187
CVE-2026-16806	150.49.8.187
CVE-2026-16807	150.49.8.187
CVE-2026-0290	148.18.4.217
CVE-2026-0289	150.49.4.125

Recommendations:

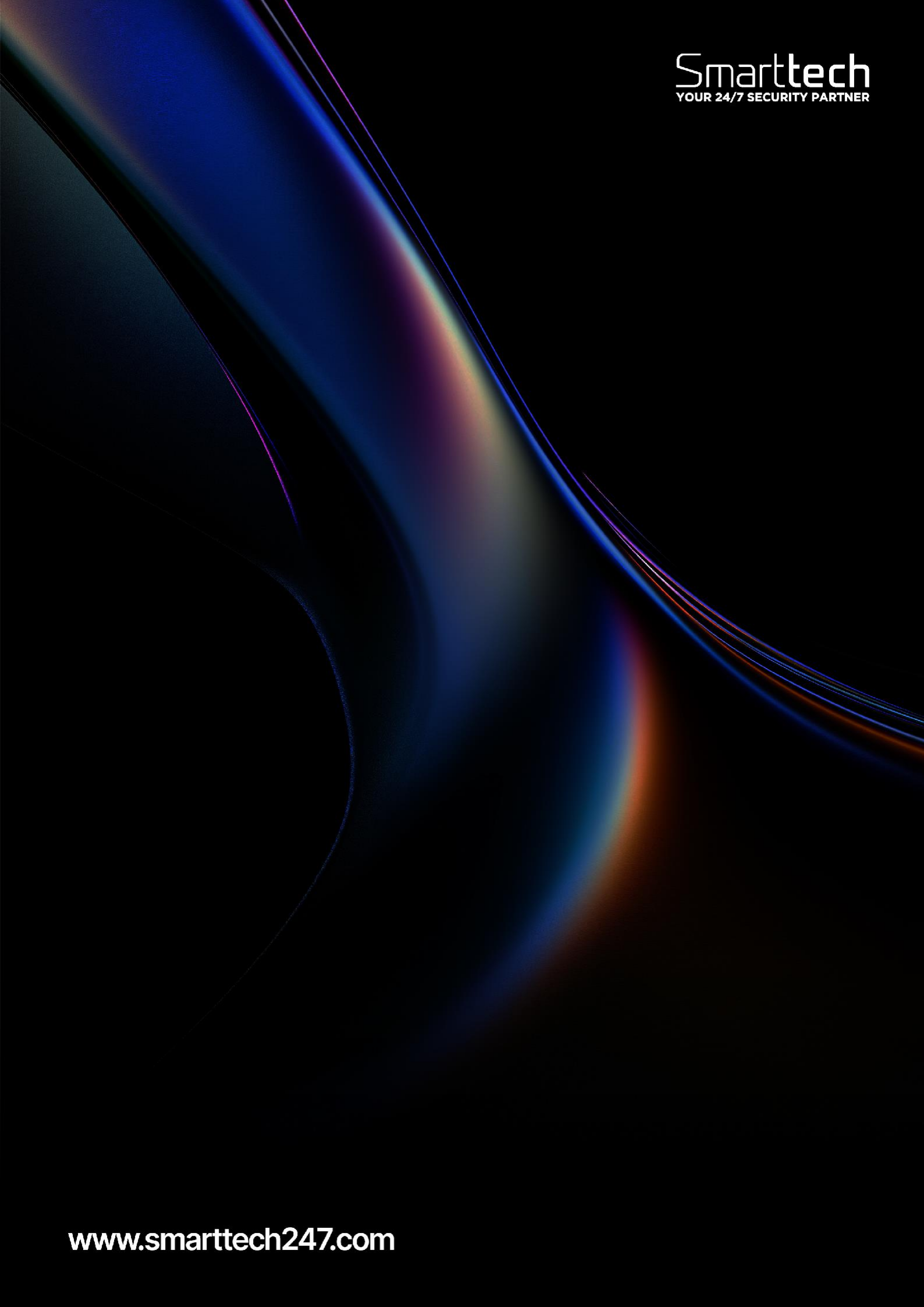
Smarttech247 team recommend the following actions to be taken:

- **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-2026-0011
https://security.paloaltonetworks.com/CVE-2026-0291
https://security.paloaltonetworks.com/CVE-2026-0292
https://security.paloaltonetworks.com/CVE-2026-0293
https://security.paloaltonetworks.com/CVE-2026-0294
https://security.paloaltonetworks.com/CVE-2026-0295
https://security.paloaltonetworks.com/CVE-2026-0296
https://security.paloaltonetworks.com/CVE-2026-0297
https://security.paloaltonetworks.com/CVE-2026-0298
https://security.paloaltonetworks.com/CVE-2026-0299
https://security.paloaltonetworks.com/CVE-2026-0301


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