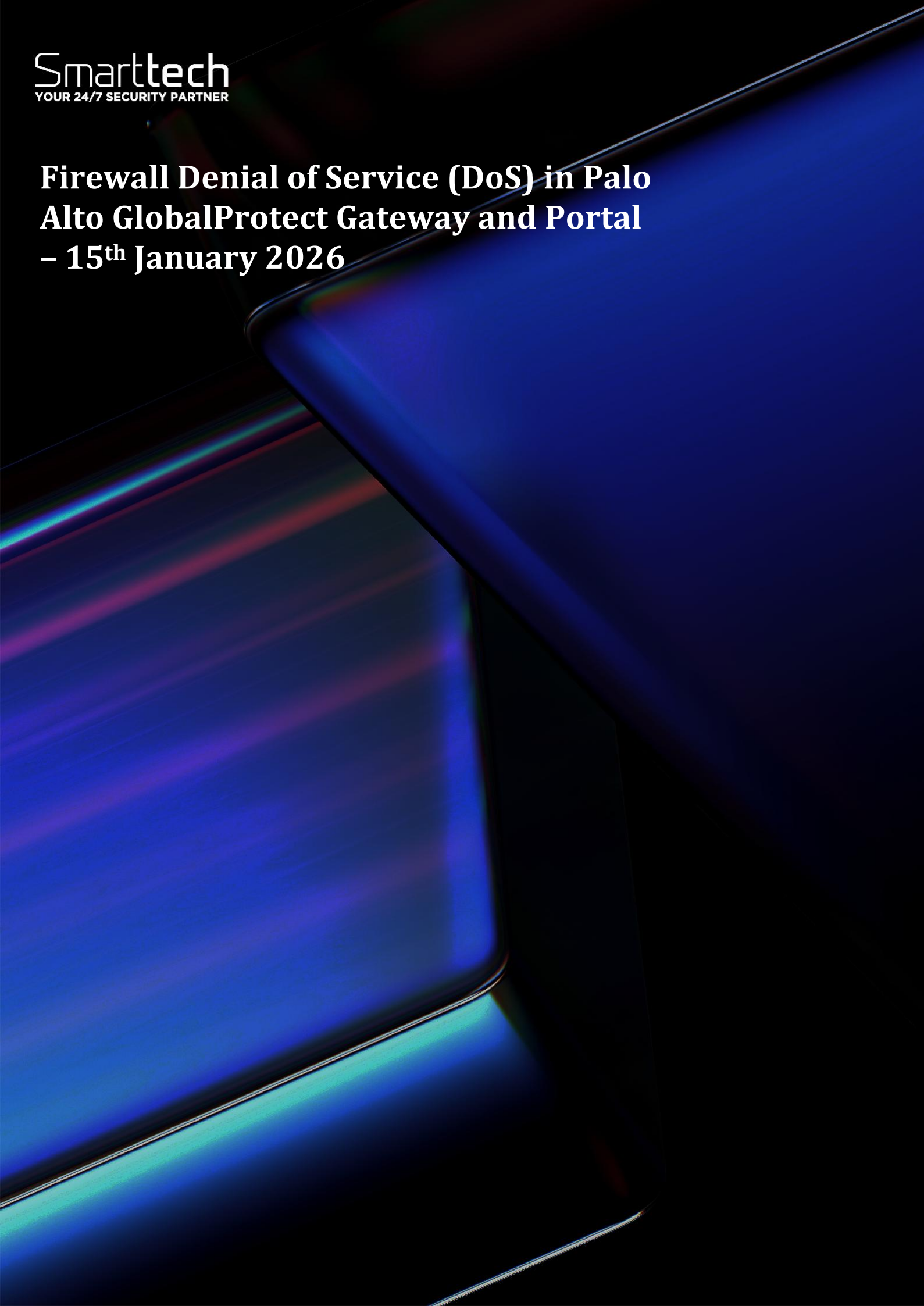
Smarttech
YOUR 24/7 SECURITY PARTNER

Firewall Denial of Service (DoS) in Palo Alto GlobalProtect Gateway and Portal – 15th January 2026



Document ID	SMA- Threat Report
Document status	ISSUED
Authors	Dorin Costantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-01-15
Issue Date	2026-01-15

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

A high severity vulnerability, CVE-2026-0227, has been identified in Palo Alto Networks PAN-OS software, specifically affecting versions 10.1, 10.2, 11.1, 11.2, and 12.1 which could lead to a denial of service (DoS) to the firewall.

Technical Summary

CVE-2026-0227 PAN-OS: Firewall Denial of Service (DoS) in GlobalProtect Gateway and Portal

CVSSv4.0 Base Score: 8.7

CVE-2026-0227 is a vulnerability in Palo Alto Networks PAN-OS software that enables an unauthenticated attacker to cause a denial of service (DoS) to the firewall. Repeated attempts to trigger this issue results in the firewall entering into maintenance mode.

Affected Products

Version	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.3-h3 < 12.1.4	>= 12.1.3-h3 >= 12.1.4
PAN-OS 11.2	< 11.2.4-h15 < 11.2.7-h8 < 11.2.10-h2	>= 11.2.4-h15 (ETA: 1/14/2026) >= 11.2.7-h8 >= 11.2.10-h2
PAN-OS 11.1	< 11.1.4-h27 < 11.1.6-h23 < 11.1.10-h9 < 11.1.13	>= 11.1.4-h27 >= 11.1.6-h23 >= 11.1.10-h9 >= 11.1.13
PAN-OS 10.2	< 10.2.7-h32 < 10.2.10-h30 < 10.2.13-h18 < 10.2.16-h6 < 10.2.18-h1	>= 10.2.7-h32 >= 10.2.10-h30 >= 10.2.13-h18 >= 10.2.16-h6 >= 10.2.18-h1

PAN-OS 10.1	< 10.1.14-h20	>= 10.1.14-h20
Prisma Access 11.2	< 11.2.7-h8*	>= 11.2.7-h8*
Prisma Access 10.2	< 10.2.10-h29*	>= 10.2.10-h29*

This issue is applicable only to PAN-OS NGFW or Prisma Access configurations with an enabled GlobalProtect gateway or portal.

Solution

Version	Minor Version	Suggested Solution
Cloud NGFW All		No action needed.
PAN-OS 12.1	12.1.0 through 12.1.3	Upgrade to 12.1.4 or later.
PAN-OS 11.2	11.2.8 through 11.2.10	Upgrade to 11.2.10-h2 or later.
	11.2.5 through 11.2.7	Upgrade to 11.2.7-h8 or 11.2.10-h2 or later.
	11.2.0 through 11.2.4	Upgrade to 11.2.4-h15 or 11.2.10-h2 or later.
PAN-OS 11.1	11.1.11 through 11.1.12	Upgrade to 11.1.13 or later.
	11.1.7 through 11.1.10	Upgrade to 11.1.10-h9 or 11.1.13 later.
	11.1.5 through 11.1.6	Upgrade to 11.1.6-h23 or 11.1.13 or later.
	11.1.0 through 11.1.4	Upgrade to 11.1.4-h27 or 11.1.13 or later.
PAN-OS 10.2	10.2.17 through 10.2.18	Upgrade to 10.2.18-h1 or later.
	10.2.14 through 10.2.16	Upgrade to 10.2.16-h6 or 10.2.18-h1 or later.
	10.2.11 through 10.2.13	Upgrade to 10.2.13-h18 or 10.2.18-h1 or later.
	10.2.8 through 10.2.10	Upgrade to 10.2.10-h30 or 10.2.18-h1 or later.
	10.2.0 through 10.2.7	Upgrade to 10.2.7-h32 or 10.2.18-h1 or later.
All older unsupported PAN-OS versions		Upgrade to a supported fixed version.
Prisma Access 11.2	11.2 through	Upgrade to 11.2.7-h8 or later.*
Prisma Access 10.2	10.2 through	Upgrade to 10.2.10-h29 or later.*

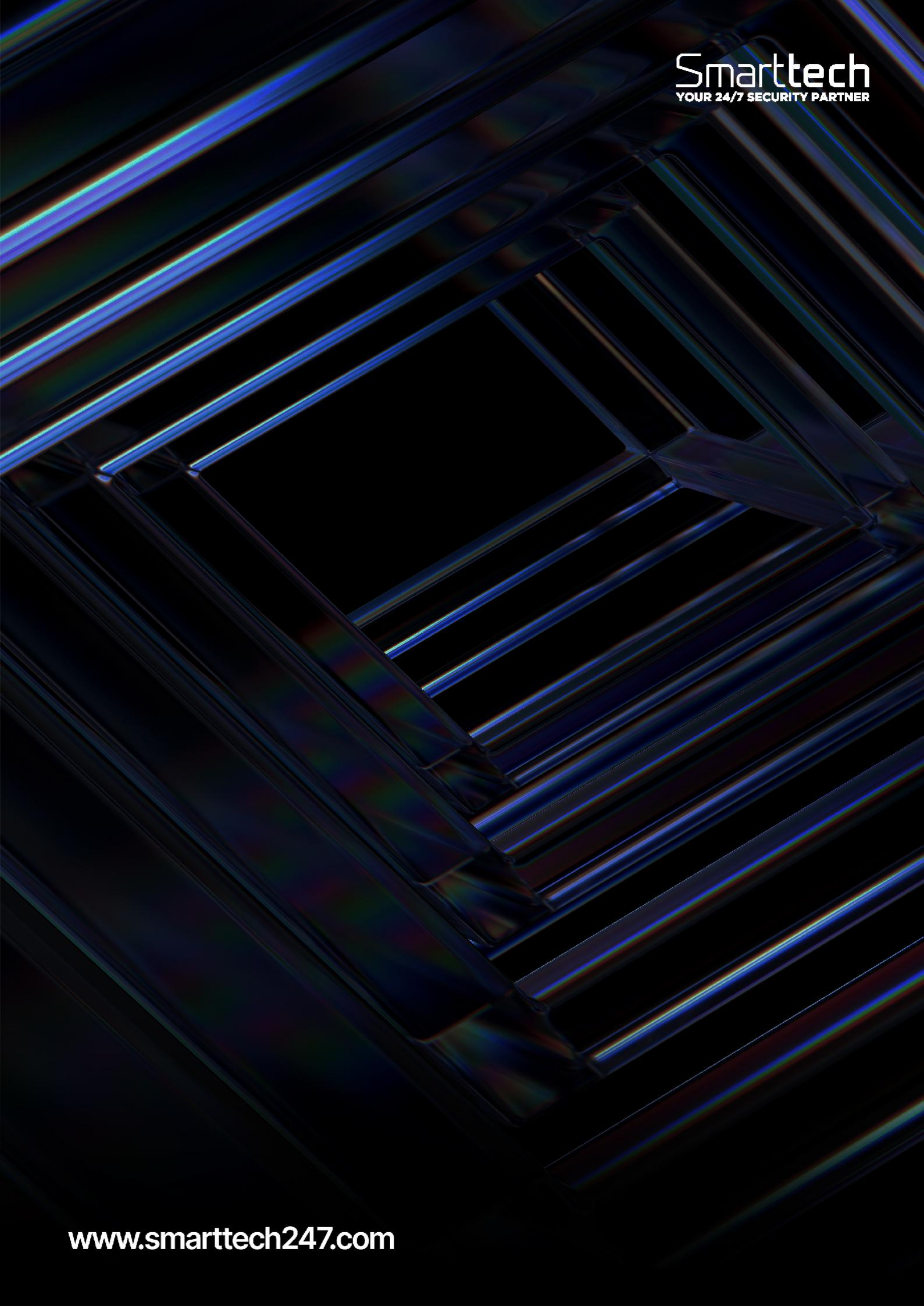
References

https://security.paloaltonetworks.com/CVE-2026-0227
https://www.paloaltonetworks.com/network-security/cloud-ngfw

https://www.paloaltonetworks.com/network-security/pan-os
https://www.paloaltonetworks.com/sase/access

CVE

CVE-2026-0227


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