Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0172

Kwetsbaarheid verholpen in Palo Alto Networks PAN-OS en Prisma Access

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 30-05-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Palo Alto Networks heeft een kwetsbaarheid verholpen in de GlobalProtect portal- en gateway-componenten van PAN-OS.

Duiding

Een ongeauthenticeerde kwaadwillende kan de kwetsbaarheid misbruiken voor het opzetten van een VPN-verbinding. Zodoende krijgt de kwaadwillende toegang tot interne systemen die via de VPN-verbinding worden aangeboden. Systemen zijn alleen kwetsbaar wanneer (HTTPS-)certificaten worden hergebruikt en de optie "Generate cookie for authentication override" of "Accept cookie for authentication override" is ingeschakeld.

Beveiligingsbedrijf Rapid7 meldt dat de kwetsbaarheid actief wordt misbruikt. Daarnaast is voor de kwetsbaarheid proof-of-conceptcode (PoC-code) publiekelijk beschikbaar. Gegeven de beschikbaarheid van de PoC-code, de algemene interesse van kwaadwillenden in edge-devices en de toegang die kwaadwillenden via deze kwetsbaarheid verkrijgen, verwacht het NCSC dat de schaal van misbruik de komende tijd toeneemt.

Oplossingen

Palo Alto Networks heeft beveiligingsupdates uitgebracht om de kwetsbaarheid te verhelpen. Het NCSC adviseert om deze updates zo spoedig mogelijk te installeren. Daarnaast adviseert het NCSC om kwetsbare omgevingen te controleren op aanwezigheid van de door Rapid7 gedeelde indicators-of-compromise (IOC's). Zie de bijgevoegde referenties voor meer informatie over de kwetsbaarheid en kwetsbare configuraties.

Referenties

- https://security.paloaltonetworks.com/CVE-2026-0257
- https://www.rapid7.com/blog/post/etr-rapid7-observed-exploitation-of-pan-os-globalprotect-authentication-bypass-vulnerability-cve-2026-0257/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-0257	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-565	Reliance on Cookies without Validation and Integrity Checking

Getroffen producten

Palo Alto Networks
PAN-OS
Prisma Access
pan-os
prisma_access

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.