



NCSC-2026-0132

Kwetsbaarheid verholpen in Palo Alto Networks PAN-OS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 06-05-2026

Revisie: 1.0.1

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

Update Revisie 1

New revision

Feiten

Palo Alto Networks heeft een kwetsbaarheid verholpen in PAN-OS, specifiek in de User-ID Authentication Portal component van PA-Series en VM-Series firewalls.

Duiding

De kwetsbaarheid betreft een buffer overflow in de User-ID Authentication Portal, waardoor niet-geauthenticeerde aanvallers willekeurige code kunnen uitvoeren met root privileges. Prisma Access, Cloud NGFW en Panorama appliances zijn niet kwetsbaar. Het is gangbare praktijk om de User-ID Authentication Portal niet direct aan het internet bloot te stellen. Exploitatie kan leiden tot volledige systeemcompromittering via de authenticatieportal.

Palo Alto heeft beperkt misbruik waargenomen, gericht op Palo Alto Networks User-ID™-authenticatieportalen die blootgesteld zijn aan niet-vertrouwde IP-adressen en/of het openbare internet. Het is niet gebruikelijk om het User-ID™-authenticatieportalal direct publiekelijk aan het internet bloot te stellen.

Oplossingen

Palo Alto Networks heeft updates uitgebracht, waaronder een workaround, om de kwetsbaarheid te verhelpen of te mitigeren. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://security.paloaltonetworks.com/CVE-2026-0300>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-0300	9.3 CRITICAL

CWE's

--

CWE	Beschrijving
> CWE-787	Out-of-bounds Write

Getroffen producten

Palo Alto Networks
PAN-OS

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.