



# NCSC-2025-0220

## Kwetsbaarheden verholpen in Palo Alto PAN-OS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-07-2025

### **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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Palo Alto Networks heeft kwetsbaarheden verholpen in PAN-OS.

## Duiding

De kwetsbaarheden omvatten een informatielek in de SD-WAN functie, waardoor ongeautoriseerde gebruikers pakketten kunnen onderscheppen en onbeveiligde gegevens van de firewall kunnen benaderen. Dit vormt een risico voor gevoelige informatie die wordt verzonden. Daarnaast is er een command injection kwetsbaarheid die geauthenticeerde beheerders in staat stelt om systeembeperkingen te omzeilen en willekeurige commando's uit te voeren als root-gebruiker, wat toegang tot de PAN-OS CLI vereist. Deze kwetsbaarheid kan worden geëxploiteerd via de beheerswebinterface, wat benadrukt dat geauthenticeerde toegang noodzakelijk is. Cloud NGFW en Prisma® Access zijn niet getroffen door deze kwetsbaarheden.

## Oplossingen

Palo Alto Networks heeft patches uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- <https://security.paloaltonetworks.com/CVE-2025-4229>
- <https://security.paloaltonetworks.com/CVE-2025-4230>
- <https://security.paloaltonetworks.com/CVE-2025-4231>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-4229</a>	6.0 MEDIUM
➤ <a href="#">CVE-2025-4230</a>	8.4 HIGH
➤ <a href="#">CVE-2025-4231</a>	8.6 HIGH

## CWE's

CWE	Beschrijving
> <a href="#">CWE-497</a>	Exposure of Sensitive System Information to an Unauthorized Control Sphere
> <a href="#">CWE-77</a>	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> <a href="#">CWE-78</a>	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

## Getroffen producten

PaloAlto 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.