



# NCSC-2025-0058

## Kwetsbaarheden verholpen in Palo Alto Networks PAN-OS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 21-02-2025

Revisie: 1.0.2

### **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)

## Update Revisie 2

GrayNoise geeft aan dat CVE-2025-0108 actief wordt misbruikt.

## Feiten

Palo Alto Networks heeft kwetsbaarheden verholpen in PAN-OS.

## Duiding

De kwetsbaarheden omvatten een authenticatie-bypass die ongeauthenticeerde kwaadwillenden in staat stelt om specifieke PHP-scripts aan te roepen via de management webinterface, een ongeauthenticeerde bestandsverwijdering die kwaadwillenden in staat stelt om specifieke bestanden te verwijderen, en een command injection kwetsbaarheid die geauthenticeerde beheerders in staat stelt om willekeurige commando's uit te voeren als de 'openconfig' gebruiker. Deze kwetsbaarheden kunnen leiden tot gegevensverlies, systeeminstabiliteit en een significante bedreiging voor de integriteit van het systeem.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de management-interface. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separate beheeromgeving.

Er vind inmiddels actief misbruik plaats van CVE-2025-0108, die ongeauthenticeerde kwaadwillenden in staat stelt om specifieke PHP-scripts aan te roepen via de management webinterface.

Update: er is publieke proof-of-concept code beschikbaar voor de kwetsbaarheid met kenmerk CVE-2025-0110.

## Oplossingen

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

## Referenties

- <https://security.paloaltonetworks.com/CVE-2025-0108>
- <https://security.paloaltonetworks.com/CVE-2025-0110>
- <https://security.paloaltonetworks.com/CVE-2025-0109>
- <https://www.greynoise.io/blog/greynoise-observes-active-exploitation-of-pan-os-authentication-bypass-vulnerability-cve-2025-0108#>

## Kwetsbaarheden

CVE	CVSS Score
> <a href="#">CVE-2025-0108</a>	8.8 HIGH
> <a href="#">CVE-2025-0109</a>	6.9 MEDIUM
> <a href="#">CVE-2025-0110</a>	8.6 HIGH

## CWE's

CWE	Beschrijving
> <a href="#">CWE-306</a>	Missing Authentication for Critical Function
> <a href="#">CWE-78</a>	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> <a href="#">CWE-73</a>	External Control of File Name or Path

## Getroffen producten

<b>palo_alto_networks</b>
cloud_ngfw
pan-os_openconfig_plugin
prisma_access
<b>paloaltonetworks</b>
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.