Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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
CVE-2025-4229	6.0 MEDIUM
CVE-2025-4230	8.4 HIGH
CVE-2025-4231	8.6 HIGH

CWE's

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

Getroffen producten

PaloAlto Networks
PAN-OS

Disclaimer