Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0227

Kwetsbaarheden verholpen in Palo Alto Networks PAN-OS

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-07-2026

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 meerdere kwetsbaarheden verholpen in PAN-OS software, specifiek in PA-Series en VM-Series firewalls, evenals Panorama management platforms.

Duiding

De kwetsbaarheden betreffen verschillende onderdelen van PAN-OS.

- Er zijn meerdere cross-site scripting (XSS) kwetsbaarheden in de User-ID Authentication Portal, GlobalProtect gateway/portal en Clientless VPN modules, die ongeauthenticeerde aanvallers in staat stellen om willekeurige JavaScript-code uit te voeren.
- Een IPv6-pakketverwerkingsfout maakt het mogelijk om firewall security policies te omzeilen, waardoor toegang tot normaal beschermde services mogelijk is.
- Een informatielek laat een ongeauthenticeerde aanvaller met netwerktoegang tot de management webinterface toe om sessietokens te verkrijgen via een kwaadaardige link.
- Daarnaast bestaat er een kwetsbaarheid waardoor ongeauthenticeerde aanvallers bestanden kunnen verwijderen uit een tijdelijke map via de management webinterface.
- De Large Scale VPN (LSVPN) feature kent een authenticatie-omzeilingsfout, waarmee onbevoegden site-to-site VPN-verbindingen kunnen opzetten, en een XML-injectie die kan leiden tot ongeautoriseerde informatietoegang of datacorruptie.
- Een server-side request forgery (SSRF) kwetsbaarheid maakt het mogelijk voor geauthenticeerde beheerders om ongeautoriseerde verzoeken naar interne services te sturen.
- Verder is er een command injection kwetsbaarheid in de management plane die geauthenticeerde beheerders root-toegang tot het besturingssysteem kan geven.
- Meerdere denial of service (DoS) kwetsbaarheden kunnen door ongeauthenticeerde aanvallers een firewall in onderhoudsmodus dwingen, wat de normale werking verstoort.
- Tenslotte zijn er buffer overflow kwetsbaarheden in de User-ID Terminal Server Agent die DoS of remote code execution mogelijk maken.

De Cloud NGFW en Prisma Access producten zijn niet getroffen door deze kwetsbaarheden. Beperking van toegang tot de management interface tot vertrouwde interne IP-adressen vermindert het risico op exploitatie.

Oplossingen

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

Referenties

- https://security.paloaltonetworks.com/json/CVE-2026-0279
- https://security.paloaltonetworks.com/json/CVE-2026-0280
- https://security.paloaltonetworks.com/json/CVE-2026-0281
- https://security.paloaltonetworks.com/json/CVE-2026-0282
- https://security.paloaltonetworks.com/json/CVE-2026-0283
- https://security.paloaltonetworks.com/json/CVE-2026-0284
- https://security.paloaltonetworks.com/json/CVE-2026-0285
- https://security.paloaltonetworks.com/json/CVE-2026-0286
- https://security.paloaltonetworks.com/json/CVE-2026-0287
- https://security.paloaltonetworks.com/json/CVE-2026-0288

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-0279	1.3 LOW
CVE-2026-0280	1.7 LOW
CVE-2026-0281	2.1 LOW
CVE-2026-0282	2.7 LOW
CVE-2026-0283	4.5 MEDIUM
CVE-2026-0284	4.7 MEDIUM
CVE-2026-0285	4.7 MEDIUM
CVE-2026-0286	6.0 MEDIUM
CVE-2026-0287	6.6 MEDIUM
CVE-2026-0288	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation

CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-131	Incorrect Calculation of Buffer Size
CWE-306	Missing Authentication for Critical Function
CWE-524	Use of Cache Containing Sensitive Information
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-787	Out-of-bounds Write
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Palo Alto Networks
PAN-OS
Panorama

Disclaimer