Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2025-0004

Kwetsbaarheden verholpen in SonicWall SonicOS

2025-01-08 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Sonicwall heeft kwetsbaarheden verholpen in SonicOS voor Gen6 en Gen7 firewalls.

Interpretaties

De eerste kwetsbaarheid betreft een zwakke pseudo-willekeurige getallengenerator in de SSLVPN (CVE-2024-40762), waardoor aanvallers in sommige gevallen authenticatietokens kunnen voorspellen. CVE-2024-53704 betreft een onjuiste authenticatie in de SSLVPN, waardoor externe aanvallers de authenticatie kunnen omzeilen. CVE-2024-53705 betreft een server-side request forgery kwetsbaarheid in de SSH-beheerinterface, die TCP-verbindingen naar willekeurige IP-adressen toestaat. Tot slot betreft CVE-2024-53706 een lokale privilege-escalatie kwetsbaarheid in het Gen7 SonicOS Cloud-platform, waardoor laaggeprivilegieerde op afstand geauthenticeerde aanvallers roottoegang kunnen verkrijgen en mogelijkerwijze willekeurige code uit kunnen voeren.

Oplossingen

Sonicwall heeft updates uitgebracht voor de getroffen systemen om de kwetsbaarheden te verhelpen. Ook adviseert Sonicwall om toegang tot de management interface en de SSLVPN te beperken tot vertrouwde infrastructuren en accounts te voorzien van Tweefactor-authenticatie. Specefieke kwetsbare hardware versies welke kwetsbaar zijn staan vernoemd in de Sonicwall advisory, SNWLID-2025-0003. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003