



NCSC-2025-0004

Kwetsbaarheden verholpen in SonicWall SonicOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 18-02-2025

Revisie: 1.0.1

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

Update Revisie 1

Onderzoekers hebben Proof-of-Concept-code (PoC) vrijgegeven, waarmee de kwetsbaarheid kan worden aangetoond.

Feiten

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

Duiding

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 mogelijk willekeurige code uit kunnen voeren.

Onderzoekers hebben Proof-of-Concept-code (PoC) gepubliceerd waarmee de kwetsbaarheid met kenmerk CVE-2024-53704 kan worden aangetoond. Succesvol misbruik vereist dat er minstens één actieve VPN-sessie aanwezig is op het kwetsbare systeem. De kwaadwillende kan dan die sessie overnemen, maar heeft niet voldoende controle om de sessie open te houden wanneer de gebruiker de VPN-verbinding verbreekt, of de mogelijkheid zelf een nieuwe sessie op te bouwen. Succesvol misbruik en eventuele vervolgschade is dus afhankelijk van de tijd die de kwaadwillende krijgt in de actieve sessie en de rechten van het slachtoffer.

De PoC is dermate eenvoudig van opzet, tevens worden er meldingen waargenomen van actief misbruik.

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. Specifieke 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>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2024-53704	9.8 CRITICAL
> CVE-2024-53705	8.6 HIGH
> CVE-2024-40762	9.8 CRITICAL
> CVE-2024-53706	

CWE's

CWE	Beschrijving
> CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
> CWE-918	Server-Side Request Forgery (SSRF)
> CWE-269	Improper Privilege Management
> CWE-287	Improper Authentication

Getroffen producten

sonicwall
sonicos
ssl_vpn

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.