Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0353

Kwetsbaarheid verholpen in Sonicwall SonicOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-09-2024
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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 2

Het NCSC ontvangt signalen dat ransomware actoren misbruik lijken te maken van deze kwetsbaarheid.

Feiten

Sonicwall heeft een kwetsbaarheid verholpen in SonicOS voor Gen5, Gen6 en Gen7 firewalls.

Duiding

De kwetsbaarheid bevindt zich in de management interface en de SSLVPN en stelt een kwaadwillende in staat om een Denial-of-Service te veroorzaken en mogelijk toegang te krijgen tot systeemgegevens en deze aan te passen.

Van betrouwbare partners ontvangt het NCSC signalen dat ransomware groepen zich al langere tijd specifiek concentreren op kwetsbaarheden in SonicOS-systemen en dat deze kwetsbaarheid misbruikt lijkt te worden om toegang te krijgen tot de infrastructuur en ransomware uit te rollen. Indicaties geven aan dat de kwetsbaarheid wordt misbruikt via de SSLVPN, waarbij met name lokale accounts worden gecompromitteerd, indien tweefactor-authenticatie (MFA) niet in gebruik is.

Oplossingen

Sonicwall heeft updates uitgebracht voor de getroffen systemen om de kwetsbaarheid 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. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-40766	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-284	Improper Access Control

Getroffen producten

sonicwall
sonicos
sonicwall_sonicos__5.9.2.14-13o
sonicwall_sonicos__6.5.2.8-2n
sonicwall_sonicos__6.5.4.15.116n
sonicwall_sonicos__7.0.1-5035

Disclaimer