Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0145

Kwetsbaarheden verholpen in SonicWall SMA100

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-05-2025

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

SonicWall heeft kwetsbaarheden verholpen in de SMA100 serie.

Duiding

De kwetsbaarheden bevinden zich in de manier waarop de SMA100 serie omgaat met geauthenticeerde SSLVPN-gebruikers. CVE-2025-32819 stelt deze gebruikers in staat om pad-traversal-controles te omzeilen en willekeurige bestanden te verwijderen, wat kan leiden tot een reset van het apparaat naar de fabrieksinstellingen. CVE-2025-32820 maakt het mogelijk om pad-traversal-sequenties te exploiteren, waardoor elke directory beschrijfbaar wordt. CVE-2025-32821 staat geauthenticeerde SSLVPN-beheerders toe om shell-commando-argumenten voor bestandsuploads in te voegen.

Het is mogelijk dat kwaadwillenden de kwetsbaarheden in keten kunnen misbruiken om een kwetsbaar systeem te resetten naar fabrieksinstellingen en over te nemen. Voor succesvol misbruik moet de kwaadwillende echter wel over geldige SSLVPN gebruikerscredentials beschikken.

Oplossingen

SonicWall heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0011

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-32819	8.8 HIGH
CVE-2025-32820	8.8 HIGH
CVE-2025-32821	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-552	Files or Directories Accessible to External Parties
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Getroffen producten

SonicWall
SMA100

Disclaimer