Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0464

Kwetsbaarheden verholpen in SonicWall SMA100 SSLVPN

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 06-12-2024

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 SSLVPN (Specifiek voor firmware versies 10.2.1.13-72sv en eerder).

Duiding

De kwetsbaarheden in de SonicWall SMA100 SSLVPN omvatten een heap-gebaseerde buffer overflow, een stack-gebaseerde buffer overflow, en een probleem met de certificaatvereiste tijdens authenticatie. Deze kwetsbaarheden kunnen door remote geauthenticeerde aanvallers worden misbruikt om willekeurige code uit te voeren op de getroffen systemen, wat kan leiden tot ongeautoriseerde toegang en controle over gevoelige gegevens. Daarnaast is er een zwakte in de pseudo-willekeurige getallengenerator (PRNG) die de integriteit van SSLVPN-verbindingen in gevaar kan brengen.

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-2024-0018

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-38475	
CVE-2024-40763	
CVE-2024-45318	
CVE-2024-45319	
CVE-2024-53702	
CVE-2024-53703	

CWE's

CWE	Beschrijving
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
CWE-116	Improper Encoding or Escaping of Output
CWE-798	Use of Hard-coded Credentials
CWE-284	Improper Access Control
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow

Getroffen producten

sonicwall
sma100
sma100_firmware

Disclaimer