



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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
➤ <a href="#">CVE-2024-38475</a>	
➤ <a href="#">CVE-2024-40763</a>	
➤ <a href="#">CVE-2024-45318</a>	
➤ <a href="#">CVE-2024-45319</a>	
➤ <a href="#">CVE-2024-53702</a>	
➤ <a href="#">CVE-2024-53703</a>	

## CWE's

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

## Getroffen producten

<b>sonicwall</b>
sma100
sma100_firmware

## 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.