Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0471

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in SonicOS van SonicWall

Publicatiedatum: 09-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

SonicWall heeft zeven kwetsbaarheden verholpen in SonicOS voor Gen7- en Gen8-firewalls.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-19868 heeft een CVSS-score van 7.1 en betreft een fout in de authenticatiehandhaving binnen de SSL-VPN-functionaliteit. Een kwaadwillende met geldige inloggegevens voor een alternatieve authenticatiemethode kan de kwetsbaarheid op afstand misbruiken om de SAML-authenticatie te omzeilen. Hierdoor kan ook multifactorauthenticatie (MFA), die via SAML wordt afgedwongen, worden omzeild. SonicWall heeft onderzoek gedaan naar meldingen van mogelijk actief misbruik. Inmiddels is de kwetsbaarheid ook opgenomen in de Known Exploited Vulnerabilities-catalogus van CISA.

De kwetsbaarheden met kenmerken CVE-2026-107154 en CVE-2026-107155 hebben beide een CVSS-score van 8.8 en betreffen respectievelijk een fout in de sessievalidatie en een onjuist beveiligd cross-domain-beleid in de beheerinterface van SonicOS. Een niet-geauthenticeerde kwaadwillende kan deze kwetsbaarheden onder specifieke omstandigheden op afstand misbruiken om ongeautoriseerde handelingen uit te voeren. Hierbij is wel gebruikersinteractie vereist.

De kwetsbaarheid met kenmerk CVE-2026-82308 heeft een CVSS-score van 7.5 en betreft een heap-based buffer overflow in de SSL-VPN-functionaliteit. Een niet-geauthenticeerde kwaadwillende kan deze kwetsbaarheid op afstand misbruiken om een Denial-of-Service (DoS) te veroorzaken.

De overige drie kwetsbaarheden betreffen twee buffer-overflows in de TACACS+-authenticatiefunctionaliteit en een zwakke wachtwoordhashing op virtuele SonicOS-appliances. Misbruik van de buffer-overflows kan leiden tot verstoring van de dienstverlening. De zwakke wachtwoordhashing kan een kwaadwillende met bestaande lokale toegang in staat stellen een platformcredential te achterhalen.

Oplossingen

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

Referenties

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0014

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-19703	8.8 HIGH
CVE-2026-19868	8.8 HIGH
CVE-2026-77708	8.8 HIGH
CVE-2026-77709	8.8 HIGH
CVE-2026-82308	8.8 HIGH
CVE-2026-107154	8.8 HIGH
CVE-2026-107155	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-291	Reliance on IP Address for Authentication
CWE-308	Use of Single-factor Authentication
CWE-798	Use of Hard-coded Credentials
CWE-916	Use of Password Hash With Insufficient Computational Effort
CWE-942	Permissive Cross-domain Security Policy with Untrusted Domains

Getroffen producten

SonicWall
SonicOS
SonicOS SSLVPN

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.