



Advisory NCSC-2026-0403

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in SonicWall SMA1000 Appliance

Publicatiedatum: 07-10-2026

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 delen. 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 meerdere kwetsbaarheden verholpen in de SonicWall SMA1000 Appliance.

Duiding

De kwetsbaarheden omvatten een pre-authenticatie Server-Side Request Forgery (SSRF) die ongeauthenticeerde aanvallers in staat stelt om onbevoegde interne verzoeken uit te voeren. Daarnaast is er een post-authenticatie remote code execution kwetsbaarheid via OS command injection. Verder is er een Zip Slip kwetsbaarheid in de management console die het mogelijk maakt om bestanden buiten de bedoelde directories te extraheren. Tot slot is er een stored Cross-Site Scripting (XSS) kwetsbaarheid aanwezig in de management console. Deze kwetsbaarheden beïnvloeden de kernbeveiligingsmechanismen van het apparaat en kunnen worden misbruikt om de integriteit en vertrouwelijkheid van het systeem aan te tasten. De kwetsbaarheden bevinden zich zowel in pre- als post-authenticatie contexten.

Oplossingen

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

Referenties

- <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0017>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-102258	10.0 CRITICAL
CVE-2026-102257	10.0 CRITICAL
CVE-2026-102255	10.0 CRITICAL
CVE-2026-102256	10.0 CRITICAL

CWE's

CWE	Beschrijving
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')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-441	Unintended Proxy or Intermediary ('Confused Deputy')
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

sonicwall
SMA1000

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 or 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.