



NCSC-2026-0239

Zero-Day kwetsbaarheden verholpen in SonicWall SMA1000

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 15-07-2026

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 twee kwetsbaarheden verholpen in SonicWall SMA1000 appliances.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-15409 betreft een Server-Side Request Forgery (SSRF) in de Work Place interface, waarmee een niet-geauthenticeerde aanvaller het apparaat verzoeken kan laten sturen naar ongewenste locaties.

De kwetsbaarheid met kenmerk CVE-2026-15410 is een post-authenticatie code-injectie in de Appliance Management Console (AMC), waardoor een geauthenticeerde aanvaller met admin rechten willekeurige OS-commando's op het apparaat kan uitvoeren.

Beide kwetsbaarheden zijn als zero-days misbruikt. Het NCSC raadt organisaties aan de advisory van SonicWall op te volgen, de aanwezigheid te controleren van de bijgevoegde IoC's en de aanbevolen acties uit te voeren.

Oplossingen

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

Referenties

➤ <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-15409	10.0 CRITICAL
➤ CVE-2026-15410	9.4 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-94	Improper Control of Generation of Code ('Code Injection')

[> 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 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.