Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0337

Zero-Day kwetsbaarheden verholpen in SMA1000 Appliance van SonicWall

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 02-09-2026

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 kwetsbaarheden verholpen in de SMA1000 Appliance.

Duiding

De SMA1000 Appliance bevat twee kwetsbaarheden. De eerste is een pre-authenticatie Server-Side Request Forgery (SSRF) in de Work Place interface, waarmee een externe, niet-geauthenticeerde aanvaller ongeautoriseerde acties kan uitvoeren. De tweede kwetsbaarheid betreft post-authenticatie remote code execution, waarbij een aanvaller met geldige inloggegevens willekeurige code op afstand kan uitvoeren.

Beide kwetsbaarheden zijn als zero-days misbruikt. Het NCSC raadt organisaties aan de advisory van SonicWall op te volgen

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-2026-0016

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-83548	10.0 CRITICAL
CVE-2026-83549	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-441	Unintended Proxy or Intermediary ('Confused Deputy')

CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

SonicWall
SMA1000
SonicWall SMA 1000 Series Firmware

Disclaimer