Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0296

Kwetsbaarheid verholpen in WatchGuard Fireware OS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-10-2025
Revisie: 1.0.1

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

Update Revisie 1

Update naar aanleiding van onderzoek van CVE-2025-9242

Feiten

Onderzoekers hebben data gepubliceerd over waar de kwetsbaarheid zich zeer waarschijnlijk bevind, het is de verwachting dat naar aanleiding van deze publicatie er op korte termijn Proof of Concept code beschikbaar komt, waarmee uitbuiting van de kwetsbaarheid zeer waarschijnlijk wordt.

Duiding

De kwetsbaarheid bevindt zich in de manier waarop Fireware OS omgaat met Out-of-bounds Write. Dit stelt een kwaadwillende, ongeauthenticeerde aanvaller in staat om willekeurige code uit te voeren. Dit kan leiden tot ernstige gevolgen voor de getroffen systemen met specifieke VPN-configuraties.

Oplossingen

WatchGuard heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Voor bepaalde situaties waarin updaten niet direct mogelijk is heeft WatchGuard mitigerende maatregelen beschikbaar gesteld. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00015

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-9242	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-787	Out-of-bounds Write

Getroffen producten

WatchGuard
Firebox
Fireware OS

Disclaimer