Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0400

Kwetsbaarheid verholpen in WatchGuard Firebox

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 19-12-2025

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

Er is een kwetsbaarheid verholpen in WatchGuard Fireware OS.

Duiding

Er is een kwetsbaarheid verholpen in WatchGuard Fireware OS. De kwetsbaarheid CVE-2025-14733 betreft een out-of-bounds write in het iked-proces van Fireware OS en treft zowel de Mobile User VPN (IKEv2) als de Branch Office VPN (IKEv2) wanneer deze is geconfigureerd met een dynamische gateway-peer. De kwetsbaarheid stelt een niet-geauthenticeerde aanvaller op afstand in staat om willekeurige code uit te voeren.

Als de WatchGuard Firebox eerder is geconfigureerd met een Mobile User VPN (IKEv2) of Branch Office VPN (IKEv2) naar een dynamische gateway-peer, en beide configuraties inmiddels zijn verwijderd, kan het systeem alsnog kwetsbaar zijn indien er nog steeds een Branch Office VPN naar een statische gateway-peer is geconfigureerd.

WatchGuard heeft pogingen tot misbruik van de kwetsbaarheid waargenomen.

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.

Controleer de omgeving op aanwezigheid van de indicatoren genoemd door beveiligingsbedrijf WatchGuard, die kunnen namelijk duiden op misbruik van de kwetsbaarheid. Bij aanwezigheid van de IOC's adviseert WatchGuard om alle lokaal opgeslagen secrets op kwetsbare Firebox apparaten te roteren. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-14733	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-787	Out-of-bounds Write

Getroffen producten

WatchGuard
Fireware OS

Disclaimer