



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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 bevindt, 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
➤ <a href="#">CVE-2025-9242</a>	<b>9.3 CRITICAL</b>

## CWE's

CWE	Beschrijving
➤ <a href="#">CWE-787</a>	Out-of-bounds Write

## Getroffen producten

<b>WatchGuard</b>
Firebox
Fireware OS

## 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.