



# NCSC-2026-0335

## Kwetsbaarheden verholpen in WatchGuard Fireware OS

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 01-09-2026

**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](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)

## Feiten

WatchGuard heeft kwetsbaarheden verholpen in WatchGuard Fireware OS, specifiek in het iked-proces en de epm-service van het Mobile Security onderdeel.

## Duiding

De kwetsbaarheden bevinden zich in het iked-proces en de epm-service van WatchGuard Fireware OS. Het iked-proces bevat een stack-based buffer overflow, een type confusion kwetsbaarheid en een heap overflow. Deze kwetsbaarheden kunnen worden misbruikt door een ongeauthenticeerde aanvaller door speciaal vervaardigd netwerkverkeer te verzenden. Dit kan leiden tot het uitvoeren van willekeurige code met de privileges van het iked-proces, waardoor volledige controle over het systeem mogelijk kan worden.

Daarnaast bevat de epm-service, die onderdeel is van het verouderde Mobile Security-component, een stack-based buffer overflow. Ook deze kwetsbaarheid kan door een ongeauthenticeerde aanvaller worden misbruikt om willekeurige code uit te voeren en daarmee controle over het systeem te verkrijgen.

## Oplossingen

WatchGuard heeft updates uitgebracht om de kwetsbaarheden in Fireware OS te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- <https://psirt.watchguard.com/CVE-2026-13086>
- <https://psirt.watchguard.com/CVE-2026-19313>
- <https://psirt.watchguard.com/CVE-2026-19315>
- <https://psirt.watchguard.com/CVE-2026-19318>

## Kwetsbaarheden

| CVE                              | CVSS Score   |
|----------------------------------|--------------|
| ➤ <a href="#">CVE-2026-19318</a> | 9.3 CRITICAL |
| ➤ <a href="#">CVE-2026-19315</a> | 9.3 CRITICAL |
| ➤ <a href="#">CVE-2026-19313</a> | 9.3 CRITICAL |
| ➤ <a href="#">CVE-2026-13086</a> | 9.3 CRITICAL |

CWE's

| CWE       | Beschrijving                                                           |
|-----------|------------------------------------------------------------------------|
| > CWE-120 | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') |
| > CWE-121 | Stack-based Buffer Overflow                                            |
| > CWE-122 | Heap-based Buffer Overflow                                             |
| > CWE-125 | Out-of-bounds Read                                                     |
| > CWE-129 | Improper Validation of Array Index                                     |
| > CWE-190 | Integer Overflow or Wraparound                                         |
| > CWE-191 | Integer Underflow (Wrap or Wraparound)                                 |
| > CWE-763 | Release of Invalid Pointer or Reference                                |
| > CWE-787 | Out-of-bounds Write                                                    |
| > CWE-798 | Use of Hard-coded Credentials                                          |
| > CWE-843 | Access of Resource Using Incompatible Type ('Type Confusion')          |

Getroffen producten

|                |
|----------------|
| WatchGuard     |
| Firebox        |
| Fireware<br>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.