



Advisory NCSC-2026-0404

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in WatchGuard Fireware OS

Publicatiedatum: 07-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

WatchGuard heeft meerdere kwetsbaarheden verholpen in Fireware OS.

Duiding

De impact van deze kwetsbaarheden varieert, net als de toegangsrechten die nodig zijn voor misbruik.

- Een aanvaller met schrijfrechten op het systeem kan via een kwetsbaarheid in SAML single sign-on-sessies een kwaadaardig sessiebestand laden en arbitraire code uitvoeren.
- Geauthenticeerde beheerders kunnen via path traversal in de WebUI Management Agent willekeurige lokale bestanden lezen. Een low-privileged geauthenticeerde gebruiker kan via resource-uitputting van diagnostische tools een denial-of-service veroorzaken.
- De spamBlocker-service bevat een stack-based buffer overflow die door een geauthenticeerde beheerder kan leiden tot een crash of code-executie.
- Een stack-based buffer overflow in de DHCP fingerprinting-daemon kan door een niet-geauthenticeerde aanvaller met netwerktoegang worden misbruikt voor code-executie of een crash.
- Een geauthenticeerde gebruiker met beperkte Access Portal-rechten kan via een SAML-login kwetsbaarheid ongeautoriseerde toegang tot Mobile VPN with SSL verkrijgen.
- Een remote, niet-geauthenticeerde aanvaller kan via resource-uitputting in het wgagent-loginproces een denial-of-service veroorzaken.
- De Access Portal reverse proxy bevat een improper authorization-kwetsbaarheid waardoor geauthenticeerde gebruikers met beperkte rechten toegang kunnen krijgen tot ongeautoriseerde webapplicaties.
- Een NULL pointer dereference in de NetFlow-packetverwerking kan door een remote, niet-geauthenticeerde aanvaller een crash veroorzaken.
- De BOVPN Over TLS-clientconfiguratie bevat een code-injection-kwetsbaarheid waardoor een aanvaller die de remote VPN-server beheert commando's met rootrechten kan uitvoeren op het Firebox-apparaat.
- Integer-underflow kwetsbaarheden in de IKE- en IKEv2-daemons kunnen door remote, niet-geauthenticeerde aanvallers worden misbruikt om crashes en daarmee denial-of-service te veroorzaken.
- Een NULL pointer dereference in het authenticatieproces kan door een remote, niet-geauthenticeerde aanvaller een crash van de managementdaemon veroorzaken.
- Een OS command injection in de interne API van WatchGuard Access Points kan door een aanvaller met netwerktoegang worden misbruikt voor het uitvoeren van willekeurige commando's.
- Een CSRF-kwetsbaarheid in WatchGuard Dimension kan het mogelijk maken om zonder toestemming database snapshots te creëren.
- Een missing authorization-kwetsbaarheid in de wgagent Management API kan door geauthenticeerde gebruikers met beperkte rechten worden misbruikt voor ongeautoriseerde API-verzoeken, crashes en het lezen van willekeurige bestanden.

- Een kwetsbaarheid in libxml2 kan leiden tot een out-of-bounds read en denial-of-service bij het verwerken van XML-input.

Oplossingen

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

Referenties

- <https://psirt.watchguard.com/>
- <https://psirt.watchguard.com/CVE-2026-13046>
- <https://psirt.watchguard.com/CVE-2026-13224>
- <https://psirt.watchguard.com/CVE-2026-13225/>
- <https://psirt.watchguard.com/CVE-2026-18105>
- <https://psirt.watchguard.com/CVE-2026-18145>
- <https://psirt.watchguard.com/CVE-2026-18146/>
- <https://psirt.watchguard.com/CVE-2026-81433>
- <https://psirt.watchguard.com/CVE-2026-86101>
- <https://psirt.watchguard.com/CVE-2026-86102/>
- <https://psirt.watchguard.com/CVE-2026-86104>
- <https://psirt.watchguard.com/CVE-2026-86105>
- <https://psirt.watchguard.com/CVE-2026-86106/>
- <https://psirt.watchguard.com/CVE-2026-86128>
- <https://psirt.watchguard.com/CVE-2026-86131>
- <https://psirt.watchguard.com/CVE-2026-86132>
- <https://psirt.watchguard.com/CVE-2026-86133>
- <https://psirt.watchguard.com/CVE-2026-86134>
- <https://psirt.watchguard.com/CVE-2026-86135/>
- <https://psirt.watchguard.com/CVE-2026-86136>
- <https://psirt.watchguard.com/CVE-2026-86137/>
- <https://psirt.watchguard.com/CVE-2026-90441>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-13046	7.5 HIGH
CVE-2026-13224	8.2 HIGH
CVE-2026-13225	5.3 MEDIUM
CVE-2026-18105	7.1 HIGH
CVE-2026-18145	8.6 HIGH
CVE-2026-18146	7.2 HIGH
CVE-2026-81433	8.7 HIGH
CVE-2026-86101	7.2 HIGH
CVE-2026-86102	9.3 CRITICAL
CVE-2026-86104	8.7 HIGH
CVE-2026-86105	6.0 MEDIUM
CVE-2026-86106	8.7 HIGH
CVE-2026-86128	8.2 HIGH
CVE-2026-86131	9.2 CRITICAL
CVE-2026-86132	8.2 HIGH
CVE-2026-86133	8.2 HIGH
CVE-2026-86134	8.7 HIGH
CVE-2026-86135	7.0 HIGH
CVE-2026-86136	7.1 HIGH
CVE-2026-86137	2.9 LOW
CVE-2026-90441	7.1 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23	Relative Path Traversal
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-176	Improper Handling of Unicode Encoding
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-295	Improper Certificate Validation
CWE-409	Improper Handling of Highly Compressed Data (Data Amplification)
CWE-476	NULL Pointer Dereference
CWE-502	Deserialization of Untrusted Data
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-1284	Improper Validation of Specified Quantity in Input

Getroffen producten

WatchGuard
Fireware
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 or 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.