Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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
CVE-2026-19318	9.3 CRITICAL
CVE-2026-19315	9.3 CRITICAL
CVE-2026-19313	9.3 CRITICAL
CVE-2026-13086	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 OS

Disclaimer