



Advisory NCSC-2026-0430

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Juniper Networks Junos OS

Publicatiedatum: 16-10-2026

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

Juniper heeft meerdere kwetsbaarheden verholpen in Junos OS.

Duiding

De kwetsbaarheden bevinden zich in verschillende componenten van Junos OS, waaronder de VXLAN Gateway Daemon (vgd), kmd op MX Series routers, SDK service met JDAF routing, TWAMP client (rmopd service), gRPC library, ipfd daemon op SRX Series, dot1x daemon op Fusion Aggregation Devices, routing protocol daemon (rpd) op MX Series, jdhcpd process, authd process, kernel bij Extended Echo, pkid component, UTM Anti-Spam SBL component op SRX Series, J-Web management interface, en srxpfe component op SRX Series met chassis-cluster configuratie.

Een aanvaller kan deze kwetsbaarheden misbruiken door het versturen van speciaal vervaardigde pakketten of berichten, vaak zonder authenticatie, wat kan leiden tot crashes van processen of het gehele systeem, denial of service, of in sommige gevallen uitvoering van arbitraire code met root privileges.

De kwetsbaarheden zijn specifiek gebonden aan bepaalde functies of configuraties binnen Junos OS, zoals het gebruik van Security Intelligence feeds, dot1x synchronisatie, HFRR link protection, DHCP client operaties, RADIUS authenticatie, Extended Echo feature, CMP enrollment, Anti-Spam SBL inspectie, J-Web interface, en chassis-cluster fabric traffic. Sommige kwetsbaarheden kunnen worden misbruikt door een aanvaller binnen het netwerk of door een gecompromitteerde externe entiteit zoals een SDN-controller of een RADIUS server.

Oplossingen

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

Referenties

- <https://supportportal.juniper.net/s/article/2026-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-SRX-Series-Multiple-vulnerabilities-resolved>
- <https://supportportal.juniper.net/s/article/2026-10-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-resolved>
- <https://supportportal.juniper.net/s/article/2026-10-Security-Bulletin-Junos-OS-MX-Series-Multiple-vulnerabilities-resolved>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-103994	8.7 HIGH
CVE-2026-102182	9.3 CRITICAL
CVE-2026-102176	8.7 HIGH
CVE-2026-102070	9.2 CRITICAL
CVE-2026-102072	7.1 HIGH
CVE-2026-102062	9.2 CRITICAL
CVE-2026-102069	8.7 HIGH
CVE-2026-102063	7.1 HIGH
CVE-2026-102057	8.7 HIGH
CVE-2026-102014	8.7 HIGH
CVE-2026-101980	9.3 CRITICAL
CVE-2026-101973	8.7 HIGH
CVE-2026-101955	9.2 CRITICAL
CVE-2026-101956	9.3 CRITICAL
CVE-2026-101937	7.1 HIGH

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-134	Use of Externally-Controlled Format String
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-195	Signed to Unsigned Conversion Error
CWE-409	Improper Handling of Highly Compressed Data (Data Amplification)

CWE	Beschrijving
CWE-476	NULL Pointer Dereference
CWE-617	Reachable Assertion

Getroffen producten

Juniper
Junos OS
Junos OS Evolved

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.