Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0224

Kwetsbaarheden verholpen in Juniper Networks Junos OS en Junos OS Evolved

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-07-2026

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

Juniper heeft meerdere kwetsbaarheden verholpen in Junos OS en Junos OS Evolved, specifiek voor MX Series, PTX Series, QFX Series, EX Series, SRX Series en QFX10000 Series apparaten.

Duiding

De kwetsbaarheden betreffen verschillende componenten binnen Junos OS en Junos OS Evolved, waaronder de packet forwarding engine, routing protocol daemon, management daemon, SNMP daemon, http-gatekeeper, TCP proxy plugin, IKE daemon, fileio library, SIP plugin, URL filtering plugin en CLI. Exploitatie kan leiden tot geheugenbeschadiging, crashes van processen zoals mgd, rpd, flow processing daemon, l2ald, en FPC, wat resulteert in Denial-of-Service (DoS) condities. Sommige kwetsbaarheden kunnen door lokale gebruikers met beperkte rechten worden misbruikt om code uit te voeren of processen te laten crashen. Andere kwetsbaarheden kunnen door niet-geauthenticeerde aanvallers via netwerkverkeer worden misbruikt om processen te laten crashen, informatie te lekken, licentie-uitputting te veroorzaken of firewallregels te omzeilen. Specifieke hardwaremodellen en softwareversies zijn getroffen, zoals MX Series met SPC3, SRX Series, EX Series (EX2300, EX4000, EX4100, EX4400), QFX Series, PTX Series en QFX10000 Series. Sommige kwetsbaarheden vereisen handmatige herstart van systemen of processen om normale werking te herstellen. De problemen zijn aanwezig in versies voorafgaand aan de gepubliceerde patches en updates.

Oplossingen

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

Referenties

- https://supportportal.juniper.net/JSA110072
- https://supportportal.juniper.net/JSA110073
- https://supportportal.juniper.net/JSA110074
- https://supportportal.juniper.net/JSA110075
- https://supportportal.juniper.net/JSA110076
- https://supportportal.juniper.net/JSA110077
- https://supportportal.juniper.net/JSA110078
- https://supportportal.juniper.net/JSA110079
- https://supportportal.juniper.net/JSA110080
- https://supportportal.juniper.net/JSA110081
- https://supportportal.juniper.net/JSA110082
- https://supportportal.juniper.net/JSA110083
- https://supportportal.juniper.net/JSA110084

- https://supportportal.juniper.net/JSA110085
- https://supportportal.juniper.net/JSA110086
- https://supportportal.juniper.net/JSA110087
- https://supportportal.juniper.net/JSA110088
- https://supportportal.juniper.net/JSA110089
- https://supportportal.juniper.net/JSA110090
- https://supportportal.juniper.net/JSA110091
- https://supportportal.juniper.net/JSA110092
- https://supportportal.juniper.net/JSA110093

Kwetsbaarheden

CVE	CVSS Score
CVE-2020-7450	7.8 HIGH
CVE-2026-21901	6.7 MEDIUM
CVE-2026-33794	8.2 HIGH
CVE-2026-33799	8.7 HIGH
CVE-2026-33800	7.1 HIGH
CVE-2026-33801	7.1 HIGH
CVE-2026-33802	6.8 MEDIUM
CVE-2026-33803	6.9 MEDIUM
CVE-2026-57019	7.1 HIGH
CVE-2026-57020	7.1 HIGH
CVE-2026-57021	6.9 MEDIUM
CVE-2026-57022	8.2 HIGH
CVE-2026-57023	8.7 HIGH
CVE-2026-57024	6.9 MEDIUM
CVE-2026-57025	6.8 MEDIUM

CVE-2026-57026	8.7 HIGH
CVE-2026-57027	7.1 HIGH
CVE-2026-57028	6.9 MEDIUM
CVE-2026-57029	6.0 MEDIUM
CVE-2026-57030	8.2 HIGH
CVE-2026-57031	5.3 MEDIUM
CVE-2026-57032	7.1 HIGH
CVE-2026-57054	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-236	Improper Handling of Undefined Parameters
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-466	Return of Pointer Value Outside of Expected Range
CWE-476	NULL Pointer Dereference
CWE-606	Unchecked Input for Loop Condition
CWE-694	Use of Multiple Resources with Duplicate Identifier
CWE-706	Use of Incorrectly-Resolved Name or Reference
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-787	Out-of-bounds Write
CWE-820	Missing Synchronization
CWE-862	Missing Authorization
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints

CWE-1284	Improper Validation of Specified Quantity in Input
CWE-1286	Improper Validation of Syntactic Correctness of Input

Getroffen producten

Juniper Networks
Junos OS
Junos OS Evolved

Disclaimer