



Advisory NCSC-2026-0462

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Juniper Networks Session Smart Router en Session Smart Conduc- tor

Publicatiedatum: 30-10-2026

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 Juniper Networks Session Smart Router en Session Smart Conductor.

Duiding

De kwetsbaarheden betreffen verschillende componenten van de Juniper Networks Session Smart Router en Session Smart Conductor.

- Er zijn out-of-bounds read- en write-fouten in HTTP-parser, TCP proxy, TCP header verwerking en VRRPv3 packet verwerking, die kunnen leiden tot service crashes, geheugenbeschadiging, sessie desynchronisatie en mogelijke informatielekken.
- Een improper initialisatieprobleem in de beveiligingspolicy kan leiden tot het gebruik van onjuiste encryptiesleutels, wat decryptie van netwerkverkeer of denial of service kan veroorzaken.
- Verder kunnen lokale aanvallers door speciaal vervaardigde directorynamen onbedoeld bestanden unmounten tijdens service cleanup, wat de beschikbaarheid beïnvloedt.
- Ongeauthenticeerde API endpoints maken het mogelijk voor lokale niet-geprivilegieerde gebruikers om als root willekeurige bestanden te overschrijven.
- Onvoldoende verificatie van data-integriteit in de model cache directory kan leiden tot het uitvoeren van willekeurige code en privilege escalatie.
- In de AccessManager module is er een OS command injection mogelijk via ongeldige invoer bij het verwijderen van auditregels, wat ook het verwijderen van bestanden mogelijk maakt.
- Onjuiste bestandspermissies in de RoutingManager module van Session Smart Conductor kunnen lokale gebruikers toegang geven tot gevoelige routinggegevens.
- Ongefilterde invoer in request body parameters maakt HTTP response splitting mogelijk.
- De AutomatedProvisioner van Session Smart Conductor bevat een kwetsbaarheid die ongeauthenticeerde remote command execution als root toestaat via speciaal vervaardigde salt minion IDs.
- In de ConfigDirector component kunnen geauthenticeerde REST gebruikers via ongesaniteerde invoer in certificaat- en private key API's willekeurige bestandsoperaties uitvoeren, waaronder lezen, overschrijven en verwijderen.
- Een stack buffer overflow in de DHCP client van Session Smart Router kan leiden tot remote code execution.
- Een onbeveiligde interne endpoint in Session Smart Router maakt het mogelijk voor ongeauthenticeerde aanvallers om administratieve privileges te verkrijgen.
- Een integer overflow in de Deep Packet Inspection certificate scanner kan een denial of service veroorzaken bij het inspecteren van TLS certificaten.
- Een integer underflow in de DhcpMessageDecoder kan leiden tot informatielekken en service crashes.

- Tenslotte kunnen in de AccessManager component met config-write rechten OS command injection en privilege escalatie plaatsvinden door onvoldoende validatie en neutralisatie van invoer in YANG configuraties.

Oplossingen

Juniper heeft updates uitgebracht om de kwetsbaarheden in Juniper Networks Session Smart Router en Session Smart Conductor te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://supportportal.juniper.net/s/article/2026-10-On-Demand-Security-Bulletin-Session-Smart-Router-and-Session-Smart-Conductor-Multiple-internally-discovered-vulnerabilities-resolved>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-103390	5.3 MEDIUM
CVE-2026-103391	5.3 MEDIUM
CVE-2026-103392	4.8 MEDIUM
CVE-2026-103393	4.3 MEDIUM
CVE-2026-103394	3.7 LOW
CVE-2026-103400	5.5 MEDIUM
CVE-2026-103401	8.8 HIGH
CVE-2026-103402	8.8 HIGH
CVE-2026-103403	8.8 HIGH
CVE-2026-103404	6.8 MEDIUM
CVE-2026-103405	5.8 MEDIUM
CVE-2026-103406	9.8 CRITICAL
CVE-2026-103407	8.8 HIGH

CVE	CVSS Score
CVE-2026-103408	8.8 HIGH
CVE-2026-103409	9.8 CRITICAL
CVE-2026-103410	7.5 HIGH
CVE-2026-103411	7.1 HIGH
CVE-2026-106079	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-306	Missing Authentication for Critical Function
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-787	Out-of-bounds Write
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')

Getroffen producten

Juniper Networks
Session Smart Conductor
Session Smart Router

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.