Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0006

Kwetsbaarheden verholpen in Juniper JunOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-01-2025

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 kwetsbaarheden verholpen in JunS (Specifiek voor JunOS en JunOS Evolved).

Duiding

De kwetsbaarheden bevinden zich in de manier waarop Juniper's JunOS en JunOS Evolved omgaan met BGP-pakketten en IPv6-pakketten. De eerste kwetsbaarheid kan worden misbruikt door ongeauthenticeerde aanvallers die vervormde BGP-pakketten verzenden, wat kan leiden tot een crash van de routing protocol daemon (rpd). Dit vereist een gevestigde BGP-sessie, wat het een significante zorg maakt voor de netwerkstabiliteit. De tweede kwetsbaarheid in de Juniper Tunnel Driver laat ongeauthenticeerde aanvallers toe om vervormde IPv6-pakketten te verzenden, wat kan resulteren in geheugenuitputting en daaropvolgende systeemcrashes, met impact op de stabiliteit van de getroffen systemen.

Oplossingen

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

Referenties

- https://supportportal.juniper.net/JSA92867
- https://supportportal.juniper.net/JSA92869

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-21598	7.5 HIGH
CVE-2025-21599	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-125	Out-of-bounds Read

Getroffen producten

juniper_networks
junos_os
junos_os_evolved
juniper
junos

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 of 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.