Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0073

Kwetsbaarheid verholpen in Juniper Junos OS Evolved

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-02-2026

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 een kwetsbaarheid verholpen in Junos OS Evolved (Specifiek voor PTX Series apparaten).

Duiding

De kwetsbaarheid bevindt zich in het On-Box Anomaly detection framework van Junos OS Evolved dat draait op PTX Series apparaten. De oorzaak is een onjuiste toewijzing van rechten die ongeauthenticeerde externe aanvallers in staat stelt om code met rootprivileges uit te voeren. Deze kwetsbaarheid kan op afstand via het netwerk worden misbruikt zonder authenticatie, wat aanvallers volledige controle over het apparaat geeft.

Het On-Box Anomaly Detection-framework mag uitsluitend door interne processen via de interne routinginstantie worden benaderd en niet via een extern blootgestelde poort. Om het risico op misbruik te verkleinen heeft Juniper een oplossing beschikbaar gesteld. Toegang dient te worden beperkt tot alleen vertrouwde netwerken en hosts met behulp van toegangslijsten of firewallfilters, waarbij uitsluitend de expliciet vereiste verbindingen worden toegestaan en alle overige verbindingen worden geblokkeerd.

Als alternatief kan deze service volledig worden uitgeschakeld met het commando: **request pfe anomalies disable**.

Oplossingen

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

Referenties

› https://supportportal.juniper.net/s/article/2026-02-Out-of-Cycle-Security-Bulletin-Junos-OS-Evolved-PTX-Series-A-vulnerability-allows-a-unauthenticated-network-based-attacker-to-execute-code-as-root-CVE-2026-21902

Kwetsbaarheden

CVE	CVSS Score
› CVE-2026-21902	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-732	Incorrect Permission Assignment for Critical Resource

Getroffen producten

Juniper
JUNOS
Juniper Networks
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 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.