Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0305

Kwetsbaarheden verholpen in Juniper Networks Junos OS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-10-2025

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 Junos OS (Specifiek voor EX4600, QFX5000 Series switches en SRX4700 apparaten).

Duiding

De kwetsbaarheden in Junos OS omvatten verschillende ernstige problemen, waaronder de mogelijkheid voor ongeauthenticeerde aanvallers om Denial of Service (DoS) te veroorzaken door het versturen van speciaal vervaardigde pakketten, het manipuleren van URL-parameters, en het omzeilen van authenticatieprocessen. Dit kan leiden tot systeemcrashes, ongeautoriseerde toegang tot gevoelige gegevens, en verstoring van netwerkdiensten. De impact van deze kwetsbaarheden kan aanzienlijk zijn, vooral voor organisaties die afhankelijk zijn van Junos OS voor hun netwerkbeheer.

Oplossingen

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

Referenties

› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Juniper-Security-Director-Insufficient-authorization-for-sensitive-resources-in-web-interface-CVE-2025-59968
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Device-allows-login-for-user-with-expired-password-CVE-2025-60010
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Specific-BGP-EVPN-update-message-causes-rpd-crash-CVE-2025-60004
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-With-BGP-sharding-enabled-change-in-indirect-next-hop-can-cause-RPD-crash-CVE-2025-59962
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-ACX7024-ACX7024X-ACX7100-32C-ACX7100-48L-ACX7348-ACX7509-When-specific-valid-multicast-traffic-is-received-on-the-L3-interface-a-vulnerable-device-evo-pfemand-crashes-and-restarts-CVE-2025-59967
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-Multiple-OS-command-injection-vulnerabilities-fixed-CVE-2025-60006
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-PTX-Series-except-PTX10003-An-unauthenticated-adjacent-attacker-sending-specific-valid-traffic-can-cause-a-memory-leak-in-cfmman-leading-to-FPC-crash-and-restart-CVE-2025-52961
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-PTX-Series-When-firewall-filter-rejects-traffic-these-packets-are-erroneously-sent-to-the-RE-CVE-2025-59958
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-EX4600-Series-and-

QFX5000-Series-An-attacker-with-physical-access-can-open-a-persistent-backdoor-CVE-2025-59957
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-SRX-Series-and-MX-Series-Receipt-of-specific-SIP-packets-in-a-high-utilization-situation-causes-a-flowd-crash-CVE-2025-52960
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-SRX4700-When-forwarding-options-sampling-is-enabled-any-traffic-destined-to-the-RE-will-cause-the-forwarding-line-card-to-crash-and-restart-CVE-2025-59964
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-When-a-user-with-the-name-ftp-or-anonymous-is-configured-unauthenticated-filesystem-access-is-allowed-CVE-2025-59980
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Arbitrary-file-download-vulnerability-in-web-interface-CVE-2025-59976
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Flooding-device-with-inbound-API-calls-leads-to-WebUI-and-CLI-management-access-DoS-CVE-2025-59975
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Reflected-client-side-HTTP-parameter-pollution-vulnerability-in-web-interface-CVE-2025-59977
› https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Security-Director-Policy-Enforcer-An-unrestricted-API-allows-a-network-based-unauthenticated-attacker-to-deploy-malicious-vSRX-images-to-VMWare-NSX-Server-CVE-2025-11198

Kwetsbaarheden

CVE	CVSS Score
› CVE-2025-11198	8.5 HIGH
› CVE-2025-59968	7.7 HIGH
› CVE-2025-59975	8.7 HIGH
› CVE-2025-59976	8.7 HIGH
› CVE-2025-59977	5.4 MEDIUM
› CVE-2025-52960	8.2 HIGH
› CVE-2025-59957	7.0 HIGH
› CVE-2025-59964	9.2 CRITICAL
› CVE-2025-59980	6.9 MEDIUM
› CVE-2025-52961	7.1 HIGH

CVE-2025-59958	6.9 MEDIUM
CVE-2025-59967	7.1 HIGH
CVE-2025-60006	4.8 MEDIUM
CVE-2025-59962	6.0 MEDIUM
CVE-2025-60004	8.7 HIGH
CVE-2025-60010	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-262	Not Using Password Aging
CWE-305	Authentication Bypass by Primary Weakness
CWE-306	Missing Authentication for Critical Function
CWE-346	Origin Validation Error
CWE-400	Uncontrolled Resource Consumption
CWE-476	NULL Pointer Dereference
CWE-552	Files or Directories Accessible to External Parties
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-824	Access of Uninitialized Pointer
CWE-908	Use of Uninitialized Resource

Getroffen producten

Juniper Networks
Junos OS
Junos OS Evolved
Junos Space
Junos Space Security Director
SRX Series
Security Director
Security Director Policy Enforcer
vSRX Series

Disclaimer