Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0017

Kwetsbaarheden verholpen in Juniper Networks JunOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-01-2026

TLP:WHITE

Feiten

Juniper heeft kwetsbaarheden verholpen in Junos OS (Specifiek voor SRX en MX Series apparaten).

Duiding

De kwetsbaarheden in Junos OS omvatten verschillende problemen, waaronder clickjacking, Denial-of-Service (DoS) door malformed packets, en kwetsbaarheden die kunnen worden misbruikt door ongeauthenticeerde aanvallers. Deze kwetsbaarheden kunnen leiden tot serviceonderbrekingen, netwerkinstabiliteit en ongeautoriseerde acties door gebruikers. De technische details van deze kwetsbaarheden vereisen aandacht van beveiligingsbeheerders om de impact op hun netwerkinfrastructuur te beoordelen.

Oplossingen

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

Referenties

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-A-specifically-crafted-show-chassis-command-causes-chassisd-to-crash-CVE-2025-60007
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-BGP-update-with-a-set-of-specific-attributes-causes-rpd-crash-CVE-2025-60003
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Optional-transitive-BGP-attribute-is-modified-before-propagation-to-peers-causing-sessions-to-flap-CVE-2025-60011
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Receipt-of-specific-IS-IS-update-packet-causes-memory-leak-leading-to-RPD-crash-CVE-2026-21909
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Unix-socket-used-to-control-the-jdhcpd-process-is-world-writable-CVE-2025-59961
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Use-after-free-vulnerability-In-802-1X-authentication-daemon-can-cause-crash-of-the-dot1xd-process-CVE-2026-21908
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-When-telemetry-collectors-are-frequently-subscribing-and-unsubscribing-to-sensors-chassisd-or-rpd-will-crash-CVE-2026-21921
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-Evolved-A-Linux-kernel-vulnerability-in-the-HID-driver-allows-an-attacker-to-read-information-from-the-HID-Report-buffer-CVE-2024-50302
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-Evolved-Flapping-

management-interface-causes-MAC-learning-on-label-switched-interfaces-to-stop-CVE-2026-21911

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-EX4000-A-high-volume-of-traffic-destinated-to-the-device-leads-to-a-crash-and-restart-CVE-2026-21913
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-EX4k-Series-QFX5k-Series-In-an-EVPN-VXLAN-configuration-link-flaps-cause-Inter-VNI-traffic-drop-CVE-2026-21910
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-MX10k-Series-show-system-firmware-CLI-command-may-lead-to-LC480-or-LC2101-line-card-reset-CVE-2026-21912
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-Receipt-of-a-specifically-malformed-ICMP-packet-causes-an-FPC-restart-CVE-2026-0203
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-and-MX-Series-When-TCP-packets-occur-in-a-specific-sequence-flowd-crashes-CVE-2026-21918
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-A-specifically-malformed-GTP-message-will-cause-an-FPC-crash-CVE-2026-21914
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-If-a-specific-request-is-processed-by-the-DNS-subsystem-flowd-will-crash-CVE-2026-21920
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-MX-Series-with-MX-SPC3-or-MS-MPC-Receipt-of-multiple-specific-SIP-messages-results-in-flow-management-process-crash-CVE-2026-21905
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-Specifically-malformed-SSL-packet-causes-FPC-crash-CVE-2026-21917
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-With-GRE-performance-acceleration-enabled-receipt-of-a-specific-ICMP-packet-causes-the-PFE-to-crash-CVE-2026-21906
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-Subscribing-to-telemetry-sensors-at-scale-causes-all-FPCs-to-crash-CVE-2026-21903

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-52987	5.1 MEDIUM
CVE-2026-21907	8.2 HIGH
CVE-2025-60007	6.8 MEDIUM
CVE-2026-0203	7.1 HIGH
CVE-2026-21903	7.1 HIGH
CVE-2026-21906	8.7 HIGH

CVE-2026-21914	8.7 HIGH
CVE-2026-21917	8.7 HIGH
CVE-2026-21920	8.7 HIGH
CVE-2025-59959	6.8 MEDIUM
CVE-2025-59960	6.3 MEDIUM
CVE-2025-59961	6.8 MEDIUM
CVE-2025-60003	8.7 HIGH
CVE-2025-60011	6.9 MEDIUM
CVE-2026-21908	7.5 HIGH
CVE-2026-21909	7.1 HIGH
CVE-2026-21921	7.1 HIGH
CVE-2024-50302	5.1 MEDIUM
CVE-2026-21911	7.1 HIGH
CVE-2026-21913	8.7 HIGH
CVE-2026-21910	7.1 HIGH
CVE-2026-21912	6.8 MEDIUM
CVE-2026-21905	8.7 HIGH
CVE-2026-21918	8.7 HIGH

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-126	Buffer Over-read

CWE-252	Unchecked Return Value
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-415	Double Free
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-665	Improper Initialization
CWE-667	Improper Locking
CWE-682	Incorrect Calculation
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-755	Improper Handling of Exceptional Conditions
CWE-822	Untrusted Pointer Dereference
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-908	Use of Uninitialized Resource
CWE-1021	Improper Restriction of Rendered UI Layers or Frames
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-1419	Incorrect Initialization of Resource

Getroffen producten

Juniper Networks
Junos OS
Junos OS Evolved

Junos Space
Paragon Automation (Pathfinder, Planner, Insights)
Spac

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.