

## 21.2R3-S9: Software Release Notification for JUNOS Software Version 21.2R3-S9

### Alert Description

Junos Software Service Release version 21.2R3-S9 is now available for download from the Junos software download site

### Download Junos Software Service Release:

1. Go to [Junos Platforms - Download Software page](#)
2. Input your product in the "Find a Product" search box
3. From the Type/OS drop-down menu, select *Junos SR*
4. From the Version drop-down menu, select your version
5. Click the Software tab
6. Select the Install Package as need and follow the prompts

**NOTE:** Starting on August 30th, 2024, we include PR's severity with each entry. See [KB86335](#) for the definition of PR's Severity

### Solution

Junos Software service Release version 21.2R3-S9 is now available.

### 21.2R3-S9 - List of Fixed issues

PR Number	Synopsis	Category: CoS support on ACX
<a href="#">1811850</a> Minor	Traffic drops on ge interfaces configured for PTP Product-Group=junos Severity=Minor	On ACX2200 series, ge (gigabit ethernet) interfaces configured for PTP (Precision Time Protocol), after activated for the first time, traffic can experience packet drops.
PR Number	Synopsis	Category: ACX MPLS
<a href="#">1797017</a> Minor	ACX2200 l2circuit hot-standby mode fails to forward the traffic after consecutive neighbor failover and link cutover Product-Group=junos Severity=Minor	When ACX2200 deploys l2circuit with hot-standby mode, it fails to forward the traffic after a few round link cutover. Standby mode does not have such problem.
PR Number	Synopsis	Category: "agentd" software daemon
<a href="#">1732763</a> Major	The xmlproxyd crash might be observed when there are multiple collectors Product-Group=junos Severity=Major	The Xmlproxyd crash could be seen if there are multiple collectors subscribing for Xmlproxyd sensors ar flapping frequently at the rate of 90 seconds or so. The occurrence of this issue is rare. The telemetry : absent during the time Xmlproxyd crashes and restarts on its own. This time could be within 30 seconds telemetry streaming of Xmlproxyd sensors will be resumed automatically.
<a href="#">1820510</a> Major	The JTI/UDP export format prompts "gpb-sdm" as a possible completion on executing "set services analytics export-profile format gpb-?" command Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms having JTI (Junos Telemetry Interface)/UDP (User Datagram P configuration i.e. "gpb-sdm" is showing a possible completion when the command "set services analytics executed.
PR Number	Synopsis	Category: MPC Fusion SW
<a href="#">1777534</a> Major	On MX and EX platform replacing the line-cards may trigger FPC to be offlined due to unreachable destinations Product-Group=junos	On Junos MX and EX9200 platforms when replacing MPC2E-NG and EX9200-40XS with MPC3E-NG, SCBE3 ; MPC may cause new and other line cards to go offline due to unreachable destinations. This happens du not properly updated once the fabric channel bonding has changed and impacts the traffic.

	Severity=Major	
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BBE Advanced Services related issues</b>
<a href="#">1735560</a> Major	The bbe-smgd crash can be seen in a certain scenario Product-Group=junos Severity=Major	On Junos MX platforms supporting subscriber services, the bbe (broadband edge)-smgd (subscriber man) due to memory consumption which will impact subscribers from bringing up.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BBE WiFi applications/services</b>
<a href="#">1859542</a> Major	The smgd process crashes on MX Series Junos OS platforms when DHCP/PPPoE over soft-gre is configured Product-Group=junos Severity=Major	On all Junos OS MX Series platforms with Enhanced Subscriber Management enabled, the smgd (Subscrip) crashes continuously when non default routing instances are used and the instance name is less than 7 ( either DHCP (Dynamic Host Configuration Protocol) or PPPoE (Point-to-Point Protocol over Ethernet) sub) to the continuous crashing of smgd process, the subscriber sessions are affected.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BBE database related issues</b>
<a href="#">1582263</a> Minor	The deleted loopback route prefix might exist under subscriber management when the loopback IP is deleted and added in a single commit Product-Group=junos Severity=Minor	On all MX platforms, the route prefix for the deleted loopback interface might be stuck in bbe-smgd (Bi) daemon when the loopback IP address is deleted and a new loopback IP address is added in a single con) deleting the loopback IP (Internet Protocol) address in separate commits.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BBE GRES related issues</b>
<a href="#">1658091</a> Minor	Error message after expected GRES reboot Product-Group=junos Severity=Minor	The following message is logged unnecessarily on the backup RE of MX960 during GRES failover: SYSLOG System abnormally shut down The message is incorrect as this is a normal expected shutdown.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BBE interface related issues</b>
<a href="#">1629910</a> Minor	The egress traffic on non-targeted iflset of subscribers might not be forwarded correctly over targeted AE interface Product-Group=junos Severity=Minor	In subscriber traffic across links over an aggregated Ethernet (AE) interface scenario, the egress data of PPPoE/L2TP/MPLS/DHCP) attached logical interface sets (iflset, e.g. pppoe-iflset/demux-iflset) are cor) of subscriber queues respectively over one targeted-distribution enabled Layer 2 ifl of AE interface (e.g) member link/FPC of AE are flapped, the underlying ifd of the AE bundle might not be attached to iflset) forwarding function of subscribers over the AE interface (e.g. traffic redistribution/CoS scheduling reso
<a href="#">1715410</a> Major	The bbe-smgd process is seen to crash if a large scale PWHT configuration is present Product-Group=junos Severity=Major	On all MX platforms in a subscriber scenario, the bbe-smgd process is seen to crash immediately after a) if a large scale PWHT (Pseudowire Headend Termination) configuration is present.
<a href="#">1821021</a> Major	The bbe-smgd daemon memory leak will be seen when ACI VLAN parsing fails Product-Group=junos Severity=Major	On all Junos MX platforms with enhanced Subscriber services running platforms that support ACI (Agent Identifier) VLANs( Virtual Local Area Network), the 'bbe-smgd' process memory leak can be seen if unde) huge number (~ Millions of Packets) of the ACI VLAN packet fails.
<a href="#">1850562</a> Major	Host unreachable from the router with PPPoE when "routing-service" and "RPF-check" are enabled, and the route is learned via EBGp Product-Group=junos Severity=Major	On Junos platforms configured with BGP (Border Gateway Protocol) and rpf-check over PPPoE (PPP over) unable to reach the hosts present in the routing table when these are learnt by EBGp. This issue affects
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BBE routing</b>

<a href="#">1826324</a> Critical	The subscribers get stuck post GRES switchover Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms configured with subscriber management with GRES (Graceful subscribers will not come up after an ungraceful switchover as RE0( Routing Engine) went down and FPC
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BBE state synchronization issues</b>
<a href="#">1811787</a> Critical	The process bbe-smgd crash will be observed in the Subscriber login/logout scenario Product-Group=junos Severity=Critical	On all Junos and Junos OS Evolved platforms, in a scaled stack-based Subscriber Management scenario ( etc.), the bbe-smgd process crash will be observed with continuous login/logout of a large number of s
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BBE Statistics daemon &amp; libraries</b>
<a href="#">1646846</a> Major	The bbe-statsd daemon might crash after ISSU Product-Group=junos Severity=Major	On all MX platforms with the subscriber management scenario, when ISSU happens from pre 18.4 to pos 18.4 are called preNG subscribers. For any of the preNG subscribers, if the ipv4/ipv6 family interface g
<a href="#">1720978</a> Minor	The bbe-statsd process crash is observed on the backup RE immediate after GRES was disabled Product-Group=junos Severity=Minor	On all MX platforms, a core file on the back-up RE is seen while disabling GRES. This core file will not ir issue will recover by restarting the process on its own.
<a href="#">1820001</a> Critical	Multiple processes on both the REs are crashing Product-Group=junos Severity=Critical	On Junos MX platforms, when a Stats DB corrupt entry in encountered, several processes related to sub CPU/Memory and statsd and authd both continuously crashing in both REs. As a result subscribers stuck
<a href="#">1849377</a> Major	The bbe-statsd process crash due to malformed PFE packets Product-Group=junos Severity=Major	On all MX and Junos Evolved platforms, bbe-statsd process crashes are observed in rare scenario. The is are received from PFE (Packet Forwarding Engine). The continuous crashing of bbe-statsd every 5 minut accounting functions.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Bi Directional Forwarding Detection (BFD)</b>
<a href="#">1698373</a> Critical	A few BFD sessions might flap persistently after FPC reload and stabilization Product-Group=junos Severity=Critical	On all Junos platforms and Junos Evolved with BFD sessions, FPC reload/restart might result in few BFD
<a href="#">1807182</a> Minor	Interface and protocol flaps is observed when BFD authentication is enabled Product-Group=junos Severity=Minor	On all Junos and Junos OS Evolved platforms with BFD (Bidirectional Forwarding Detection) authenticat and subsequent protocols will go down. This could result in traffic disruption for that protocol leading t
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Border Gateway Protocol</b>
<a href="#">1582411</a> Minor	CPU utilization might be increased to 100% if more than 10M BGP prefixes received Product-Group=junos Severity=Minor	In a high-scaled BGP multipath environment, if the option 'rib-group' is enabled under the BGP global le utilization. This issue could cause device performance degradation. Please refer to the workaround to a
<a href="#">1629213</a> Minor	External BGP multihop and accept-remote-nexthop feature should not be used together Product-Group=junos Severity=Minor	When you configure BGP with both EBGP "multihop" and "accept-remote-nexthop" together, it might not interface correctly upon interface flap, causing packet forwarding drops.

<a href="#">1679645</a> Minor	RSYNC session flaps between Master and Standby RE might result in errors on ephemeral commits during ISSU Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, errors might be seen on ephemeral commits during ISSU.
<a href="#">1689904</a> Major	BGP LU Advertisements fail with the message "BGP label allocation failure: Need a gateway" Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms BGP-LU (Border Gateway Protocol Labeled-Unicast) Advertise allocation failure: Need a gateway" based on timing conditions involving route resolution and installatio
<a href="#">1692320</a> Critical	Deletion and addition of BGP transport-class caused the rpd crash Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms deletion and addition of transport-class on top of BGP CT con crash seen. commit synchronization process during config commit doesn't work for auto-created routing classes.
<a href="#">1716946</a> Minor	BGP connection doesn't establish when it is configured with rfc8950-compliant under logical-systems on all Junos and Junos OS Evolved platforms Product-Group=junos Severity=Minor	BGP (Border Gateway Protocol) session/connection is not getting up and keeps flapping when rfc8950-c configured with BGP under logical-systems on all Junos and Junos OS Evolved platforms.
<a href="#">1728829</a> Minor	In a high scaled environment, high rpd CPU utilization might be observed when a routing related commit is performed Product-Group=junos Severity=Minor	On all platforms, high rpd CPU utilization might be observed when a routing related commit is performe BGP groups configured with VPN family (inet-vpn, inet6-vpn). No traffic impact or protocol flap will be utilisation will raise operational challenges, especially if the system is very scaled.
<a href="#">1729733</a> Major	BMP leads to prolonged high rpd CPU utilization upon committing the BGP peer import policy configuration Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, with BGP Monitoring Protocol (BMP) configured when a Borde policy configuration change is committed that triggers the BGP reconfiguration job for routes re-evalua (rpd) CPU utilization up to 100% will be observed for a long time which may impact routing as high rpd i
<a href="#">1737679</a> Major	The rpd crash files are seen due to a use-after free of objects Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, due to a use-after free of objects that are being shared acro when some assumptions were broken in a recent fix. The crash files generated in rare conditions when trace is cut.
<a href="#">1738074</a> Minor	BFD session for BGP remains down in a specific scenario Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms supporting BFD (Bi-directional Forwarding and Detection) for hop BFD sessions can remain in a down state. This issue is seen when the multi-hop BFD session endpoir interface addresses on which the BFD is configured are not directly connected.
<a href="#">1753233</a> Major	IBGP route dampening not working in a L3VPN scenario Product-Group=junos Severity=Major	On Junos and Junos OS Evolved platforms with L3VPN, flapping routes are not suppressed when damper family inet6-vpn unicast for internal BGP sessions.
<a href="#">1754935</a> Minor	BGP multipath route is not correctly applied after changing the IGP metric Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, multipath route is not correctly applied due to this Equal-co when Border Gateway Protocol (BGP) multipath is configured and the Interior Gateway Protocol (IGP) m subsequently reverted.
<a href="#">1761627</a> Major	Increase in task memory observed on 'clear validation database' Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when routing-options session validation is configured, and BC increases in every iteration on executing 'clear validation database' command.
<a href="#">1763095</a> Minor	BGP link bandwidth community based load balancing is not working if BGP-PIC is enabled Product-Group=junos Severity=Minor	On all Junos and Junos Evolved T640, T1600, T4000, TX Matrix, TX Matrix Plus, MX5, MX10, MX40, MX80 MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, vMX, EX4500, EX9204, EX920 when Border Gateway Protocol Prefix-Independent Convergence (BGP-PIC) is enabled, the weighted Equ as expected.
<a href="#">1785231</a>	PE Routers continue to drop prefixes in	On all Junos and Junos OS Evolved platforms configured as a Provider Edge (PE) in an L3VPN scenario pe

Minor	a L3 VPN scenario Product-Group=junos Severity=Minor	client, when there are no external BGP peers configured with a static route-target-filter as `local`, VPI dropped which is as per design and expected behavior. However, when an external BGP session is established from-main-vpn-tables' is configured, the PE doesn't flap all existing BGP sessions, and the refresh of prefixes advertised by RR continue to be dropped at PE.
<a href="#">1787290</a> Critical	Junos OS and Junos OS Evolved: Receipt of a specific malformed BGP update causes the session to reset (CVE-2024-39555) Product-Group=junos Severity=Critical	An Improper Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (RPD) of Junos OS Evolved allows an attacker sending a specific malformed BGP update message to cause the session to reset (DoS). Please refer to <a href="https://supportportal.juniper.net/JSA83015">https://supportportal.juniper.net/JSA83015</a> for more information.
<a href="#">1788543</a> Minor	BGP OutQ counter of one of the BGP peers gets stuck after system reboot/restart routing/clear bgp neighbor Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, when there is a high route churn and the system reboot/restarts, there are some values stuck in the OutQ counter of one of the peers in a group. Due to this, the route update is stuck in traffic/service impact.
<a href="#">1793714</a> Major	BGP routes may not get advertised when always-wait-for-krt-drain is configured with BGP sharding Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when 'delay-route-advertisements always-wait-for-krt-drain' is configured, the end of a record or a sequence of updates is not received in the BGP (Border Gateway Protocol) peer which is stuck. This may cause the KRT (Kernel Routing Table) queue to get stuck, thereby halting the advertisement of BGP routes.
<a href="#">1797147</a> Major	Junos OS and Junos OS Evolved: Receipt of a specific malformed BGP path attribute leads to an RPD crash (CVE-2024-47491) Product-Group=junos Severity=Major	An Improper Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (RPD) of Junos OS Evolved allows a network-based, unauthenticated attacker to cause Denial of Service (DoS). Please refer to <a href="https://supportportal.juniper.net/JSA88116">https://supportportal.juniper.net/JSA88116</a> for more information.
<a href="#">1814083</a> Critical	Junos OS and Junos OS Evolved: With BGP traceoptions enabled, receipt of specifically malformed BGP update causes RPD crash (CVE-2024-39515) Product-Group=junos Severity=Critical	An Improper Validation of Consistency within Input vulnerability in the routing protocol daemon (RPD) of Junos OS Evolved allows an unauthenticated network-based attacker sending a specifically malformed BGP packet resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service. Please refer to <a href="https://supportportal.juniper.net/JSA88099">https://supportportal.juniper.net/JSA88099</a> for more information.
<a href="#">1814289</a> Minor	The IBGP session stuck in active state with 'local-as alias AS_X' when peers have different global AS configuration Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, when "local-as alias" configuration knob is used on an IBGP session in the scenario where peers have different global AS, but the same "local-as alias".
<a href="#">1815222</a> Critical	Junos OS and Junos OS Evolved: With certain BGP options enabled, receipt of specifically malformed BGP update causes RPD crash (CVE-2024-39516) Product-Group=junos Severity=Critical	An Out-of-Bounds Read vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS Evolved allows an unauthenticated network-based attacker to send a specifically malformed BGP packet to cause RPD to crash (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service in systems with BGP traceoptions enabled. Please refer to <a href="https://supportportal.juniper.net/JSA88100">https://supportportal.juniper.net/JSA88100</a> for more information.
<a href="#">1821241</a> Critical	Junos OS and Junos OS Evolved: When BGP traceoptions are configured, receipt of malformed BGP packets causes RPD to crash (CVE-2025-21598) Product-Group=junos Severity=Critical	An Out-of-bounds Read vulnerability in Juniper Networks Junos OS and Junos OS Evolved's routing protocol daemon (RPD) allows an unauthenticated, network-based attacker to send malformed BGP packets to a device configured with BGP traceoptions, causing RPD to crash. This issue requires a BGP session to be established. This issue can propagate and multiply through vulnerable devices. Please refer to <a href="https://supportportal.juniper.net/JSA92867">https://supportportal.juniper.net/JSA92867</a> for more information.
<a href="#">1826686</a> Minor	Traffic impact due to BGP route stuck in hidden state Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, with BMP (BGP Monitoring Protocol) configured, the BGP route next hop state as 'Next hop type unusable' leading to traffic drop.
<a href="#">1828380</a> Major	Junos OS and Junos OS Evolved: Receipt of specially crafted BGP update packet causes RPD crash (CVE-2025-21602) Product-Group=junos Severity=Major	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (RPD) of Junos OS Evolved allows an unauthenticated adjacent attacker sending a specific BGP update packet to cause RPD to crash (DoS). Please refer to <a href="https://supportportal.juniper.net/JSA92872">https://supportportal.juniper.net/JSA92872</a> for more information.

<a href="#">1845169</a> Major	BGP stops advertising VPN routes to EBGPeer if static route-target-filter as local is configured Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, for MPLS L3 VPN's (Multi Protocol Label Switching L3 Virtual Network) target-filter as local is configured, BGP (Border Gateway Protocol) stops advertising VPN routes to EBGPeer
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Track PRs in BGP BMP area &amp; is part of BGP inside RPD.</b>
<a href="#">1796530</a> Major	High CPU utilization due to BMP to be running with the longest and highest run count Product-Group=junos Severity=Major	In a rare situation, BMP might fall into a loop processing rib-in RM update messages but none of the messages are processed for a long time until the BMP station state is bounced. Since BMP task has low priority, it will yield CPU if the only hog CPU when system is idle and won't block other important tasks.
<a href="#">1819305</a> Critical	BMP gets stuck and does not send data to BMP collector Product-Group=junos Severity=Critical	On all Junos OS and Junos OS Evolved platforms which supports BMP (BGP Monitoring Protocol), the BMP Station. Please refer to TSB83918 for more details.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related to Common BIOS on x86 based designs</b>
<a href="#">1715258</a> Major	On EX4400 and EX4400-24X platforms, BIOS upgrade is not getting successful via CLI Product-Group=junos Severity=Major	On EX4400 and EX4400-24X platforms, BIOS upgrade is not getting successful via CLI when the system is in a specific state
<a href="#">1746973</a> Minor	Enhancement to automatically restore LKG image from an alternate location Product-Group=junos Severity=Minor	On VMhost based platforms, if BIOS gets corrupted, LKG image is used to restore BIOS. For some reason there is no way to recover the BIOS. The usual way to reinstate the LKG is manual, but with this fix it is automatic
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BBE Remote Access Server</b>
<a href="#">1641416</a> Minor	The authd process might not report CoS shaping-rate in acct-stop message Product-Group=junos Severity=Minor	Authd doesn't report CoS-Shaping-Rate VSA in Accounting Stop messages.
<a href="#">1650243</a> Major	DHCP clients with static IP addresses binding might get disconnected Product-Group=junos Severity=Major	On all Junos platforms having static IP address binding with MAC addresses under access configuration mode
<a href="#">1665947</a> Minor	New service profile provided by Radius during re-authentication triggered by DHCP Renew packet with changed actual data rate TLVs might not be applied Product-Group=junos Severity=Minor	On the MX platform with a subscriber management environment, if a new service profile was provided during authentication triggered by the DHCP Renew packet with changed actual data rate TLVs, it may not be applied and the old profile will be removed.
<a href="#">1695956</a> Major	The interim-rate under radius-options feature is not working post implementing BBE statistics performance and scale improvements Product-Group=junos Severity=Major	On all Junos platforms interim-rate under radius-options feature missing in Broadband Edge (BBE) scenario could cause more than the configured interim-rate per second at the radius server.
<a href="#">1759048</a> Minor	Test aaa command may failure due to "Subscriber creation failed" Product-Group=junos Severity=Minor	Start from Junos 22.2R1 with flex license enabled releases, test aaa command may failure due to "Subscriber creation failed"

[1826901](#) Major The authd process crash is seen when subscriber management is enabled  
Product-Group=junos  
Severity=Major

On all Junos MX platforms, the authd process would crash if it attempts to access the subscriber management undergoing re-initialization due to a problem. Due to this, new subscriber login will be affected possibly

PR Number	Synopsis	Category: Captive Portal, Content Delivery Daemon, and Service Plugin
<a href="#">1675985</a> Minor	PFE core dump is seen when the CPCD service is modified Product-Group=junos Severity=Minor	On MX240, MX480, MX960, MX2008, MX2010, and MX2020 with MPC7E, PFE core is seen when "routing-engine based CPCD (Captive Portal Content Delivery) is moved to PIC based CPCD (si- interface to ams- interface
PR Number	Synopsis	Category: MX Platform SW - FRU Management
<a href="#">1701539</a> Major	CB2 not properly offlined upon Power Zone Failure Product-Group=junos Severity=Major	Power check periodic polling happens in chassis every 2 seconds. In this scenario, a power check is done present. Usually on the SCB0, SCB1 hosts the Routing Engine but in MX960 there are 3 SCB's and SCB2 dc offlined when there are power failures which leads to fabric errors.
<a href="#">1707976</a> Minor	Upon ISSU upgrade or system reboot or FPC restart the DAC 100G speed configured port might not come up Product-Group=junos Severity=Minor	If the ISSU upgrade, FPC restart, or system reboots, then the 100G DAC cable port link goes down intermittently hardware failing to lock onto data stream and RX CDR clock not locked.
<a href="#">1801284</a> Major	The RE switchover will not be triggered in case of clock failure on SCBE3-MX Product-Group=junos Severity=Major	On MX platforms with SCBE3-MX (MX240, MX480 and MX960) due to a hardware failure of the Control Board might not happen. This will result in the 19.4Mhz clock failure and has potential risk for chassis wide traffic ports will be impacted. If the RE switchover is done in a timely manner then the device will recover before clock from the new master.
<a href="#">1816912</a> Minor	IIC access error during commit operation cause false positive alarms in devices Product-Group=junos Severity=Minor	On Junos platforms, RE detects IIC read or write failures and triggers a minor alarm " RE1 IIC access alarm
PR Number	Synopsis	Category: Virtual-chassis platform/chassisd infrastructure PRs for MX
<a href="#">1774302</a> Major	MXVC:MPC10E can not reach VC-Mm when re1 is VC-Mm Product-Group=junos Severity=Major	MXVC:MPC10E can not reach VC-Mm when re1 is VC-Mm. The issue happens only for Linux Based cards and work fine.
<a href="#">1798681</a> Minor	CHASSISD_IFDEV_RTSLIB_FAILURE: ifdev_create: rtplib_ifdm_add failed (No such file or directory) after creating a virtual interface tunnel Product-Group=junos Severity=Minor	The error messages in question are not-service affecting and would not be noticed by regression scripts
PR Number	Synopsis	Category: MX Platform SW - UI management
<a href="#">1656702</a> Major	The lane 0 information will not be displayed when the SNMP poll is done using ifindex Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, MIB information will not be displayed for lane0.
PR Number	Synopsis	Category: MX Platform SW - ukern core dumps
<a href="#">1806787</a> Major	Partial traffic blackhole will be observed during the time of FPC crash due to interfaces not going down Product-Group=junos	On all MX2K platforms with MIC-MACSEC-MRATE MIC (Modular Interfaces Card), during an FPC (Flexible FPC) crash, traffic will be lost as the interfaces might take some time to go down.

Severity=Major

PR Number	Synopsis	Category: Class of Service
<a href="#">1593059</a> Major	Traffic drop might be observed upon deactivating/activating the target-mode using the knob "set chassis satellite-management fpc <#> target-mode" Product-Group=junos Severity=Major	On MX platforms, deactivating/activating the target-mode using the knob "set chassis satellite-manager bad state at PFE on extended ports. This will lead to traffic disruption.
<a href="#">1793588</a> Major	An error was observed while performing the interface flap by making PIC on/off Product-Group=junos Severity=Major	On all Junos and Junos OS platforms, while performing interface flap by making pic on/off, error is obs
<a href="#">1836528</a> Minor	FC id goes out of sync between the RE and PFE impacting all CoS features using FC id Product-Group=junos Severity=Minor	On all Junos and Junos Evolved Platform, forwarding-class (FC) identifier (id) goes out of sync between Forwarding Engine (PFE) when software upgrade is performed. When In Service Software Upgrade (ISSU between the RE and PFE impacting all class-of-service (CoS) features using FC id. When manual softwar ISSU) , this issue will be seen as a cosmetic display issue where the order in which the FC configuration:
PR Number	Synopsis	Category: CFM
<a href="#">1788491</a> Minor	CFM sessions configured on lt interface hosted on a few line cards will not be up Product-Group=junos Severity=Minor	On all Junos MX platforms with MPC3E NG HQoS, MPC3E NG PQ & Flex Q, MPC2E NG HQoS, MPC2E NG PQ the lt interface hosted on a few line cards will not be up.
<a href="#">1790156</a> Minor	Commit error: "Cannot set interface down action on more than one session running on interface et-x/x.x rmep x" Product-Group=junos Severity=Minor	Commit error: "Cannot set interface down action on more than one session running on interface et-x/x/ CFM IFL is deleted on single IFD.
PR Number	Synopsis	Category: L2NG Access Security feature
<a href="#">1637380</a> Minor	DHCP snooping table might fail on All Junos platforms to populate MAC address after a VLAN change Product-Group=junos Severity=Minor	On All Junos platforms, the DHCP table might fail intermittently to populate MAC address after a VLAN (Address resolution protocol) inspection not working for certain devices and DHCP snoop binding(show c removed.
PR Number	Synopsis	Category: OpenSSH and related subsystems
<a href="#">1831635</a> Minor	ACX500 / hogging CPU with ssh-keygen process using 90% of CPU Product-Group=junos Severity=Minor	ACX500 / hogging CPU with ssh-keygen process using 90% of CPU
PR Number	Synopsis	Category: OpenSSL and related subsystems
<a href="#">1815253</a> Major	Junos OS: Multiple vulnerabilities resolved in OpenSSL (CVE-2024-4741, CVE-2024-2511) Product-Group=junos Severity=Major	The OpenSSL project has published security advisories for multiple vulnerabilities. Please refer to https for more information.
PR Number	Synopsis	Category: Device Configuration Daemon

<a href="#">1777137</a> Minor	The chassis-control subsystem will not respond when fxp0 interface has static ARP configured Product-Group=junos Severity=Minor	On all Junos MX platforms, when GRES (Graceful Routing Engine Swichover) is enabled and configuration (Address Resolution Protocol) entry will result in chassis-control subsystem not responding for the mana
<a href="#">1848768</a> Major	MTU configuration is not applied from the configuration group after commit and "warning" is seen Product-Group=junos Severity=Major	When configuring MTU on interfaces through a configuration-group and commit the changes, those are i
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Firewall Filter</b>
<a href="#">1699186</a> Minor	There is no commit error when filter with "then port-mirror" and no port-mirror instance for 'family inet'. Product-Group=junos Severity=Minor	Commit checking was missing for the family inet for filter with "then port-mirror" and no port-mirroring commit error can be seen appropriately when the configuration is not proper.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Control Plane for Node Virtualization</b>
<a href="#">1685453</a> Critical	PICs on the GNF failed to come online after the chassisd restart Product-Group=junos Severity=Critical	On MX platforms supporting node-slicing (MX480, MX960, MX2010, MX2020 & MX2008) have an issue that chassisd restarts, the FPC doesn't restart as expected which causes the PIC (Physical Interface Card) to
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Ethernet OAM (LFM)</b>
<a href="#">1754637</a> Minor	Out of range "Near-end loss" percentage or jnxSoamLmCurrentStatsBackwardAvgFlr Product-Group=junos Severity=Minor	On MPC1-9 line ards, Near-end loss percentages data will not be proper every time when below conditi peer misbehaving wrt to synthetic frame Loss Measurement (SLM) testid time out 2. Near-end loss happ values in output of show oam ethernet cfm sla-iterator-statistics command.
<a href="#">1809956</a> Minor	On Junos Evolved and Junos MX platforms with MPC10E/11E/LC9600 line cards traffic drop is seen due to changes in delay measurement profile Product-Group=junos Severity=Minor	On Junos Evolved and Junos MX240/MX480/MX960/MX2008/MX10008/MX10016/MX2010/MX2020 platform and MX304 platform, with enhanced-cfm mode enabled and IFL configured with dual tag, when measur configured, packets do not get transmitted if there are further changes in the measurement-interval ar
<a href="#">1811734</a> Major	The LFM session flaps will be observed at random Product-Group=junos Severity=Major	On Junos ACX5448 & ACX710 platforms with LFM (Link-fault-management) configured in distributed mod random when the peer device has LFM configured in inline mode. This will result in traffic loss.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: EVPN control plane issues</b>
<a href="#">1651631</a> Major	EVPN-VPWS: When control-word is enabled at instance/global level and not under interface then Egress routes are deleted and added back during every commit operation. Product-Group=junos Severity=Major	For EVPN VPWS instance when control-word is enabled at global level / instance level and not enabled config change can trigger an incorrect mismatch condition between the control-word configuration on t preference of the instance based on global/instance level control word config. This triggers a false posi interface and results in Egress RT deletion and addition for all the remote peers for the remote SIDs cor
<a href="#">1679115</a> Major	EVPN Proxy ARP doesn't work for the static VTEP interface Product-Group=junos Severity=Major	On all Junos platforms, MAC-IP learning doesn't happen when ARP (Address Resolution Protocol) request End Point).
<a href="#">1692249</a>	RPD (Routing Protocol Daemon) core is	On all Junos and Junos Evolved platforms, RPD(Routing Protocol Daemon) core is observed due to remot

Minor	observed due to remote bgp routes being flashed as active routes Product-Group=junos Severity=Minor	routes if the next hop is not resolved, and when "family evpn signalling no-install" knob under bgp is co
<a href="#">1697349</a> Critical	"no-local-switching" under "instance-type evpn" is allowed Product-Group=junos Severity=Critical	"no-local-switching" under "instance-type evpn" is allowed henceforth
<a href="#">1701632</a> Minor	A config change caused a rpd crashes for the EVPN migrated instance Product-Group=junos Severity=Minor	For a Juniper MX platform that has a routing instance migrated from VPLS to EVPN, a config change aft such an instance, could result in the rpd crash. The RD change could have been trigged via CLI or auto-
<a href="#">1716310</a> Minor	IRB interface is not applicable for EVPN-VPWS instance and results in rpd process core when streaming telemetry on that IRB interface Product-Group=junos Severity=Minor	After configuring the IRB (Integrated Routing and Bridging) interface with EVPN-VPWS (Ethernet Virtual Service) and when streaming telemetry, an rpd process core is observed. The IRB interface is not applic
<a href="#">1734686</a> Major	While doing a migration from VPLS to EVPN, when any changes are done like FPC restart or device reboot, the crash is observed Product-Group=junos Severity=Major	On all Junos platforms, After migration from VPLS (Virtual Private LAN service) to EVPN (Ethernet Virtu catastrophic change or FPC (Flexible PIC Concentrator) is restarted, the crash is observed.
<a href="#">1757499</a> Major	Traffic loss will be seen in EVPN-VPWS scenario as non DF is unable to relay packets Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms when the link between DF (Designated Forwarder) and CE non-DF is unable to relay packets which will lead to a traffic drop. This issue is seen in EVPN-VPWS inst
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: EVPN Layer-2 Forwarding</b>
<a href="#">1650665</a> Minor	EVPN Proxy ARP doesn't work for the restricted feature on the IRB interface Product-Group=junos Severity=Minor	On all Junos platforms, in the EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) scenario the proxy-ar (Integrated Routing and Bridging) interface will not work as expected and impacts the traffic.
<a href="#">1715343</a> Major	Ping overlay vxlan replies Overlay-segment present even the bridge-domain has been deactivated Product-Group=junos Severity=Major	The vxlan ping overlay request is received for a certain VNI on MX and the bridge-domain associated w However the MX still responses with "Overlay-segment present" sub-code in the reply message.
<a href="#">1743913</a> Minor	IRB reachability issues may be observed in the EVPN-VXLAN environment when looped ARP comes on ESI-LAG Product-Group=junos Severity=Minor	On Junos and Junos OS Evolved platforms (except MX platforms) with EVPN-VXLAN (Ethernet VPN - Virtu traffic loop conditions, self-generated ARP packets (having physical-IRB MAC as SMAC) may come back t Such rare scenarios, when the MAC address of the IRB (Integrated Routing and Bridging) ages out and is associated MAC-IP route (IRB route) might get cleaned. This may result in IRB reachability issues as the won't have IRB information of the local VTEP and on the local VTEP, there won't be EVPN database entry local IRB towards the remote VTEPs.
<a href="#">1770407</a> Major	The l2ald crash will be seen in EVPN-MPLS scenario Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms with EVPN-MPLS configured, when a BD(Bridge Domain) is MPLS(Ethernet Virtual Private Network with Multiprotocol Label Switching) routing instance and router-crash. There is no service impact due to this issue.
<a href="#">1798683</a> Major	EVPN ARP Entries and RVTEPs are deleted on Junos and EVO Platforms when Configuring PIM Sparse Mode on ESI Interfaces enabled with both family inet and inet6 Product-Group=junos Severity=Major	EVPN ARP Entries and RVTEPs are deleted on Junos and EVO Platforms when Configuring PIM Sparse Moc family inet and inet6.

PR Number	Synopsis	Category: Control plane EVPN multicast
<a href="#">1758171</a> Major	Junos OS and Junos OS Evolved: Receiving specific traffic on devices with EVPN-VPWS with IGMP-snooping enabled will cause the rpd to crash (CVE-2024-39514) Product-Group=junos Severity=Major	An Improper Check or Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon on Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). Please see <a href="https://supportportal.juniper.net/JSA82980">https://supportportal.juniper.net/JSA82980</a> for more information.
PR Number	Synopsis	Category: EX Chassis Interface Handling
<a href="#">1702988</a> Minor	Wrong Speed value shown on the CLI "show interfaces <> ext" output Product-Group=junos Severity=Minor	This issue has no service impact. and, this is regression issue from a previous/old issue. and, this is a cosmetic issue on internal/management/logical interfaces.
PR Number	Synopsis	Category: Express PFE Services including JTI, TOE, HostPath, Jflow
<a href="#">1830575</a> Major	The dcpfe crashes when ukern_trace handle buffer size is set to 10000 Product-Group=junos Severity=Major	On all Junos platforms, the dcpfe crash is seen with a core-dcpfe dump when the ukern_trace handle buffer size is set to 10000.
PR Number	Synopsis	Category: Flow-tap software
<a href="#">1839617</a> Minor	The MX is unable to properly convert SRC/DST port value for Radius-flow-tap Lawful Intercept DTCP ADD request Product-Group=junos Severity=Minor	On MX platforms (MX104, MX80, MX40, MX10, MX5) the Radius-flow-tap Lawful Intercept Dynamic Tasking does not use the requested port ID. The traffic sent to mediation device will use an unexpected port ID in DTCP ADD request, due to which the MX is unable to properly convert Source Port / Destination Port.
PR Number	Synopsis	Category: SRX4100/SRX4200 platform software
<a href="#">1814404</a> Minor	Junos OS: SRX1500,SRX4100,SRX4200: Execution of low-privileged CLI command results in chassisd crash (CVE-2025-21596) Product-Group=junos Severity=Minor	An Improper Handling of Exceptional Conditions vulnerability in the command-line processing of Juniper SRX4100, and SRX4200 devices allows a local, low-privileged authenticated attacker executing the 'show chassis' command to cause the chassis daemon (chassisd) to crash and restart, resulting in a temporary Denial of Service (DoS). Please see <a href="https://supportportal.juniper.net/JSA92864">https://supportportal.juniper.net/JSA92864</a> for more information.
PR Number	Synopsis	Category: idp flow creation, deletion,notification, session mgr intfc
<a href="#">1826377</a> Critical	Memory leak will be observed on all SRX platforms when IDP is configured Product-Group=junos Severity=Critical	On SRX platforms with IDP (Intrusion Detection and Prevention) enabled, while processing IDP traffic a memory leak will be observed as memory depletes eventually. This issue affects the following releases: SRX7.8, SRX22.2R3-S3/4, SRX22.3R3-S3, SRX22.4R3-S2/3, SRX23.2R2, SRX23.2R2-S1 and SRX24.2R1. All other releases are not affected.
PR Number	Synopsis	Category: Libjtask for RPD tasks, scheduler, timers, memory, and slip
<a href="#">1724986</a> Minor	With BGP traceoptions configuration high CPU utilization will be observed and the rpd process may crash Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms BGP traceoptions configuration will have an impact on the CPU time to recede in spite of disabling it. It is important we enable a specific trace flag and disable it when not to perform switchover and other triggers which can add load to the CPU during traces are enabled.
PR Number	Synopsis	Category: MX Inline Jflow
<a href="#">1798466</a> Major	With scaled routes and flex-flow-sizing configured memory exhaustion will occur Product-Group=junos Severity=Major	On all Junos MX platforms with LC(Linecard) MPC (Modular Port Concentrator)4-9 installed, the Linecard memory exhaustion will be seen when Jflow is configured with the inline-services flex-flow-sizing enabled and 'flex-flow-sizing' is configured.

	lead to an FPC crash Product-Group=junos Severity=Major	configured. There will be a traffic impact due to the crash.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Kernel software for AE/AS/Container</b>
<a href="#">1751260</a> Minor	Directly connected neighbour via AE becomes unreachable if the member interfaces of AE are swapped and if one AE has VLAN and the other doesn't Product-Group=junos Severity=Minor	On MPC10E line cards based MX platforms with AE (Aggregated Ethernet) interface configured with Link subscriber management and auto-configure statement enabled, ping to neighbour fails post swapping n with VLAN configuration and the other without VLAN configuration). Traffic forwarding on respective in moved from AE having VLAN to AE not having VLAN.
<a href="#">1840734</a> Major	RLT ifl remains down after RLT unit interface configuration is modified Product-Group=junos Severity=Major	On all Junos platforms which support PS over RLT, after modifying or deleting and re-adding a logical in interface remains down and the following log messages is seen in the messages log:DCD_CONFIG_WRITE failed for an IFL ADD: File exists after configuration change.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: ISIS routing protocol</b>
<a href="#">1755864</a> Major	RPD crash due to BGP sharding and SRV6 Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when Border Gateway Protocol (BGP) rib-sharding is enabled the routing protocol process (rpd) crashes.
<a href="#">1777702</a> Minor	The rpd process crashes after multiple iterations of disable/enable ISIS protocol Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, the rpd process crashes after disabling/enabling the ISIS (Int System) protocol using the set command. The issue is seen after 2-3 hours of continuous disabling, and interval.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: jdhcpd daemon</b>
<a href="#">1668015</a> Major	The jdhcpd crash might be observed in a DHCP Relay Agent scenario Product-Group=junos Severity=Major	On all MX platforms(except MX150), the jdhcpd core might be observed if the routing-instance configur leasequery(ALQ) on a DHCPv4 or DHCPv6 relay agent is deleted from the device. It will impact the Dyna functionality during the crash.
<a href="#">1730750</a> Minor	Zombie/defunct processes related to JDHCPD processes. Product-Group=junos Severity=Minor	Zombie/defunct processes related to JDHCPD processes.
<a href="#">1740822</a> Minor	DHCP ALQ no-advertise-routes-on-backup functionality does not work in VRF for Framed-Route. Product-Group=junos Severity=Minor	DHCP ALQ no-advertise-routes-on-backup functionality does not work in VRF for Framed-Route.
<a href="#">1763331</a> Minor	DHCP-OFFER gets dropped leading to subscribers not completing the DORA process in the ALQ EVPN-VPWS without the topology-discover scenario Product-Group=junos Severity=Minor	On MX platforms in the DHCP4 (Dynamic Host Configuration Protocol) and DHCPv6 subscribers in ALQ (A VPN - Virtual Private Wire Service) without topology-discover scenario, due to incorrect GIADDR (Gateway leading to subscribers not completing the DORA (Discover, Offer, Request, Acknowledge) process. The is Service) VLAN interfaces where DHCP subscribers are landing.
<a href="#">1764483</a> Minor	High CPU utilization for bbe-smgd process in the BNG scenario Product-Group=junos Severity=Minor	On MX platforms in the Subscriber Management scenario with DHCP (Dynamic Host Configuration Protoc advertise-routes-on-backup' configured, bbe-smgd high CPU utilization will be observed which can resul coming online when the subscriber's sessions stacked over the PS (Pseudowire Subscriber) interface are loop. The issue happens when a switchover from backup to master BNG (Broadband Network Gateway) interface and route operation (ADD or DELETE) is performed.
<a href="#">1769598</a> Major	The jdhcpd proecess crash will be observed due to double free of memory allocation when DHCP ALQ is configured	On MX platforms , when DHCP ALQ ( Dynamic Host Configuration Protocol Active Lease Query ) is config enabled, the jdhcpd process crash will be observed due to double free of memory allocation. The DHCP once jdhcpd process is restarted.

	Product-Group=junos Severity=Major	
<a href="#">1775108</a> Major	DHCP ALQ subscribers may not logged out after TCP connection is removed on all Junos platforms Product-Group=junos Severity=Major	On all Junos platforms with ALQ (Active-Lease Query) enabled with DHCP(Dynamic Host Configuration Protocol) subscribers login & logout and TCP connection reset, the DHCP subscribers may not properly release DHCP Relay, leading to inaccurate IP address management and allocation for the subscribers. The subscribers who are not released.
<a href="#">1779273</a> Major	DHCPv6 Information-request packets will be dropped when it has server identifier option Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms acting as Dynamic Host Control protocol (DHCP) relay agent request packets are dropped when it has server identifier option. There will be no traffic impact however parameters by client will not be shared by servers.
<a href="#">1799888</a> Major	After L2 failover, client receives DHCP attributes from the main pool configured instead of the linked pool and linked address-assignment pool name is not synced to DHCP binding on backup BNG having ALQ in BBE subscriber management scenario Product-Group=junos Severity=Major	On all Junos MX platforms configured with primary pool, with BBE (Broadband Edge) subscriber management enabled with different DHCP (Dynamic Host Configuration Protocol)-attributes within the linked address server configured, in a corner case scenario, it is observed that when L2 (layer 2) failover happens, the and not from linked pool as it should and linked address-assignment pool name is not synced to the DHCP Network Gateway). This causes default gateway and other attributes to be wrong. So when existing CPD DHCP renew, they receive wrong DHCP default gateway and other attributes and that causes traffic drop.
<a href="#">1801142</a> Major	The client session is logging out as DHCP renewal is not successful Product-Group=junos Severity=Major	On Junos MX platforms, when Wholesale and Retail use case with asymmetric-lease-time option configured client session is logging out. There will be a service impact because client session will be re-established (Discover, Offer, Request, Acknowledgement).
<a href="#">1817227</a> Major	DHCP asymmetric-lease-time is slow processing large scale requests to terminate 64K subscribers. Product-Group=junos Severity=Major	DHCP asymmetric-lease-time code has been optimized to increase the processing speed from 20 client requests per second.
<a href="#">1818919</a> Major	jdhcpd core dumps may be seen on ALQ setups when subscriber synchronization is done Product-Group=junos Severity=Major	DHCP ALQ (Active Leasequery) Sessions go down due to core dumps in jdhcpd (Juniper DHCP Daemon). On ALQ setups when subscriber synchronization happens after the TCP (Transmission Control Protocol) connection.
<a href="#">1825998</a> Major	DHCP ALQ process crashes to recover from memory leak. Product-Group=junos Severity=Major	On all Junos platforms, In a rare scenario when memory leak happens the Dynamic Host Configuration process crashes automatically.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: jpppd daemon</b>
<a href="#">1686940</a> Minor	Subscribers will fail to negotiate the PPP session and be unable to login post-software upgrade Product-Group=junos Severity=Minor	On MX platforms with Subscriber Management configured, the subscribers will fail to negotiate the PPP unable to login when jpppd transitions from Backup to Master and does not receive all the Routing Table.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Flow Module</b>
<a href="#">1820291</a> Critical	Junos OS: SRX4600 and SRX5000 Series: Sequence of specific PIM packets causes a flowd crash (CVE-2024-47503) Product-Group=junos Severity=Critical	An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow processing daemon (f SRX4600 and SRX5000 Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service. <a href="https://supportportal.juniper.net/JSA88133">https://supportportal.juniper.net/JSA88133</a> for more information.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: SRX Firewall Authentication</b>
<a href="#">1829894</a>	Captive portal authentication fails	On all SRX platforms, when a user tries to authenticate to a captive portal to get access to resources, the

Minor	when firewall-authentication is used in conjunction with identity management services (JIMS) Product-Group=junos Severity=Minor	user is rerouted back to the captive portal with no resources access.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: High Availability/NSRP/VRRP</b>
<a href="#">1821452</a> Critical	Junos OS: SRX5000 Series: Receipt of a specific malformed packet will cause a flowd crash (CVE-2024-47504) Product-Group=junos Severity=Critical	An Improper Validation of Specific Type of Input vulnerability in the packet forwarding engine (PFE) Jun Series allows an unauthenticated, network based attacker to cause a Denial of Service (Dos). Please ref <a href="https://supportportal.juniper.net/JSA88134">https://supportportal.juniper.net/JSA88134</a> for more information.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: IPSEC/IKE VPN</b>
<a href="#">1834204</a> Major	SRX becomes unresponsive when SNMP requests are sent via the fxp0 interface immediately after a reboot Product-Group=junos Severity=Major	On all SRX platforms (except SRX1600, SRX2300, SRX4700 and SRX5000 series with SPC3 card) using the VPNs (Virtual private networks), the SRX becomes almost unresponsive impacting network when SNMP (requests for VPN information arrives from the PFE and are sent via the fxp0 interface immediately after communication) connection to the PFE is established.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Security platform jweb support</b>
<a href="#">1858466</a> Major	VPN failures on SRX due to file descriptor issue Product-Group=junos Severity=Major	On all SRX platforms, Juniper Secure Connect (JSC) clients may fail to establish a VPN session after succ concurrent connections per client IP are active. In a NATted environment, the 21st connection will fail,
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Platform infra to support jvision</b>
<a href="#">1769294</a> Critical	Junos OS: Due to a race condition AgentD process causes a memory corruption and FPC reset (CVE-2024-47494) Product-Group=junos Severity=Critical	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the AgentD process of Juniper N is already causing impact to established sessions which generates counter changes picked up by the Age move the AgentD process into a state where AgentD attempts to reap an already destroyed sensor. This corruption causing the FPC to crash which is a Denial of Service (DoS). Please refer to <a href="https://supportp information">https://supportp information</a> .
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Key Management Daemon</b>
<a href="#">1781993</a> Major	Memory leak is observed on MX series platforms that run kmd process Product-Group=junos Severity=Major	On all MX series platforms that support MS-MPC/MS-MIC cards, memory leak is observed on kmd (Key M VPN is configured with DiffieHellman group24. The issue is not seen on platforms that support iked proc outputs for CLI ipsec/ike show commands and over time kmd might crash when reach its maximum men in ipsec/vpn going down.
<a href="#">1797132</a> Major	On all Junos MX Platforms with MS-MPC/MS-MIC card used in an IPsec scenario KMD process is stuck at 100% CPU Product-Group=junos Severity=Major	On all Junos MX Platforms with MS-MPC/MS-MIC card used in an IPsec scenario KMD (Key management p The issue was occurring because there was an IPsec rule configured for which IKE SA got negotiated suc Associations) was being negotiated due to traffic, there was an entry pushed inside the pending trigger approximately at the same instance, on deactivating/deleting the same IPsec rule from the configurati rule(SA config) object. Now, when the KMD process tried to trigger the entry from pending trigger list, i IPsec rule (i.e. sa config object) which is already removed and hence it gets stuck in an infinite while l
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Layer 2 Circuit issues</b>
<a href="#">1768323</a> Minor	JUNOS and JUNOS EVO-RPD process crash under High Availability Route Engine (RE) scenarios when L2circuits are enabled Product-Group=junos Severity=Minor	Routing Protocol Daemon (RPD) process crash when l2circuits are enabled in scenarios with backup Rout
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Layer2 forwarding on EX/NTF/PTX/QFX</b>

<a href="#">1680702</a> Major	L2ald core generated after executing CLI command show l2-learning mac-move-buffer. Product-Group=junos Severity=Major	L2ald core generated after executing CLI command show l2-learning mac-move-buffer.
<a href="#">1706364</a> Minor	With MAC limit and persistent MAC learning configuration l2ald process will crash when MAC is learned through remote peers Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, l2ald (Layer 2 Address Learning Daemon) will crash if the MA configured with persistent MAC learning and MAC is learned from remote peers through ICCP (Interchas
<a href="#">1763637</a> Major	Multiple NH failed errors and BT traces in IRB observed on ISIS clear and disable/enable Product-Group=junos Severity=Major	With Scaled EVPN MPLS configuration, when there is underlay ISIS flap, transient error logs related to N cards.
<a href="#">1776782</a> Minor	Host device cannot resolve target IP's ARP when client uses virtual mac address Product-Group=junos Severity=Minor	On Junos or Junos OS Evolved platforms which supports EVPN-MPLS/EVPN-VXLAN, device will not reply t requests when source MAC (Media Access Control) of ethernet header and ARP source MAC are different mac-ip-table. Traffic drop will be seen.
<a href="#">1800944</a> Minor	In EVPN-VXLAN scenario missing destination mac address causes flooding resulting in traffic loss Product-Group=junos Severity=Minor	On all Junos and Junos OS Evolved platforms in the EVPN-VXLAN scenario, ipv4 and ipv6 traffic flooding destination MAC address.
<a href="#">1820882</a> Minor	Traffic drop is seen in an EVPN multihoming scenario when mac-pinning is enabled Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, in Ethernet VPN (EVPN) multihoming scenario with mac-pinni when the Designated Forwarder role (DF) is changed.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: lacp protocol</b>
<a href="#">1706224</a> Major	On all Junos MX Series and PTX Series routers, multiple LACP timeouts cause traffic loss due to ppsman resource starvation Product-Group=junos Severity=Major	On all MX Series and PTX Series routers running Junos OS, during congestion, the periodic packet manag fails to send protocol data units (PDUs). This could cause LACP timeout and aggregated Ethernet interfa
<a href="#">1783793</a> Major	All AEs bundles configured in Active-Standby mode for EVPN-MPLS routing-instances will flap on the first commit post a fresh system reboot Product-Group=junos Severity=Major	On all Junos MX and EX platforms with MPC family of line cards, all the Aggregated-Ethernet (AEs) bund for Ethernet Virtual Private Network-Multiprotocol Label Switching (EVPN-MPLS) routing-instances on th after a fresh system reboot.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Label Distribution Protocol</b>
<a href="#">1676551</a> Minor	LDP egress-policy for default route (0.0.0.0/0) with 'exact' option will make output label for the unrelated routes Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, when Label Distribution Protocol (LDP) egress-policy for defa option is configured, it will install the "unrelated route" prefix into inet.3 and will make an output labe protocols ldp longest-match" is not configured). When this issue happens, next-hop selection may be di will also be seen.
<a href="#">1697988</a> Minor	RPD core can be seen on the dual RE platform Product-Group=junos Severity=Minor	On all Junos and Junos Evolved dual RE(Routing Engine ) platforms rpd core can be seen on configuring

<a href="#">1763432</a> Minor	The correct optimal path may not be selected in p2mp scenario Product-Group=junos Severity=Minor	The P2MP LSP to the ingress PE may follow the path with the lowest metric.
<a href="#">1801384</a> Minor	An invalid remote neighbor address is shown for IPv6 LDP with session-protection configured Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, for targeted and non-targeted IPv6 LDP sessions, the IPv6 local address format, and session-protection is not enabled.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: JDHCP is a daemon for EVO platform to handle DHCP protocol</b>
<a href="#">1720002</a> Major	The existing DHCP server bindings will be lost after configuring the additional group in the dhcp-local-server bundle Product-Group=junos Severity=Major	On Junos Evolved ACX platforms, when an additional group in the dhcp-local-server stanza is configured, the existing DHCP server bindings will be lost.
<a href="#">1806148</a> Major	Interfaces fail to coming up on ACX EVO platforms after deleting the routing-instance with DHCPv6 and adding new configuration on same interface Product-Group=junos Severity=Major	The interfaces fail to come up on Junos OS Evolved ACX platforms when routing-instance with DHCPv6 (version 6) relay/local-server configuration, is completely deleted in a single commit and a new configuration is added.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related to Junos licensing infrastructure</b>
<a href="#">1721757</a> Major	Uncleared alarm observed when any capacity license is used and installed multiple times Product-Group=junos Severity=Major	On Junos EX and MX platforms, when any capacity license is used and installed multiple times, causes unavailability of the license.
<a href="#">1759618</a> Major	License-service crash is seen on Junos OS Evolved platforms Product-Group=junos Severity=Major	On Junos OS Evolved platforms, when license with unknown feature ID/platform reserved feature ID is used, the license keys key and then if License-service is restarted or system is rebooted or software upgrade is done, crash files are seen. This is a non service impacting issue.
<a href="#">1766515</a> Minor	A warning message is seen while installing a license key with an unknown feature Product-Group=junos Severity=Minor	On all Junos platforms, a warning message is seen when installing the license key where features don't match the license key.
<a href="#">1775463</a> Major	The RE goes into amnesiac mode upon license check validation failure Product-Group=junos Severity=Major	On all Junos and Junos Evolved Platforms, the RE (Routing Engine) goes into amnesiac mode upon rebooting the "set system license keys key <>".
<a href="#">1792672</a> Minor	License is lost on NG-RE platforms after device/routing-engine reboot Product-Group=junos Severity=Minor	On NG-RE (Next Generation Routing Engine) platforms, license is lost after restarting device/routing-engine, that service will be impacted.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Port-based link layer security services and protocols that a</b>
<a href="#">1656415</a> Minor	Device could go into amnesiac when commit check fails with macsec config. Coredump could be observed for dot1xd process due to file descriptor leaks. Product-Group=junos Severity=Minor	Following issues have been fixed by this PR, 1) Device could go into amnesiac when commit check fails to be observed for dot1xd process due to file descriptor leaks.

<a href="#">1758838</a> Minor	Allow encryption offset with XPN cipher, but may not interoperate Product-Group=junos Severity=Minor	Allowing offset configuration even for XPN cipher, for some specific deployment. This may not be inter
<a href="#">1763303</a> Minor	Port remains down after flapping or configuration change until the OAM is cleared Product-Group=junos Severity=Minor	On Junos and Junos Evolved platforms with MACsec (Media Access Control security) and LFM (Link Fault Administration, and Management) configured, after link flap or deactivate/activate "exclude-protocol l down until the OAM state is cleared.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: SW PRs for MPC10E PlatformD</b>
<a href="#">1762021</a> Major	PFE disable on certain Junos MX platforms will bring down all logical IFDs tunnel/inline services Product-Group=junos Severity=Major	On Junos MX platforms with MPC10E/MPC11E line cards, Packet Forwarding Engine (PFE) disable on pfe-service/tunnel logical (IFDs) to be marked down. Conversely, on other PFEs (than inst 0), PFE disable dc services/tunnel IFLs. Expectation is that all tunnel/services IFDs local to the pfe instance must be boug IFDs (both local and non-local) are marked down.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: MPC10E timing and synchronization</b>
<a href="#">1756317</a> Major	The clksyncd process crashes on backup RE when PTP is deactivated and activated back Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms configured with PTP in Hybrid mode of operation, when P1 change of mode from SyncE to Hybrid causes SyncE clock sources in backup RE to reset and FSM timer is the SyncE clock sources are qualified in active RE and same is propagated to backup-RE through genccfg configs are checked which is a mismatch and causes clksyncd core. This issue is a rare issue and it is do
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: MPC11 ULC fabric software related issues.</b>
<a href="#">1762114</a> Minor	Linecard loses all fabric planes when another linecard is powered off ungracefully Product-Group=junos Severity=Minor	On MX2020/MX2010/MX10K4/MX10K8 platforms and MPC11E, LC9600, LC4800 line cards , linecard loses takes all interfaces down when another linecard is powered off ungracefully .
<a href="#">1798780</a> Critical	The system goes into a bad state when an SFB ungraceful offline happens due to a fatal Interrupt Product-Group=junos Severity=Critical	On MX platforms with SFB, in case of a fatal error encountered during SFB reboot ( due to hardware issu will try to offline this SFB during bootup. At the same time, the system is busy training the fabric links i system-wide traffic impact due to the fabric not being consistent.
<a href="#">1802259</a> Critical	SFB ungraceful offline followed by master SPMB reboot results in traffic drops due to fabric Link errors Product-Group=junos Severity=Critical	On MX2020/MX2010 platforms having SFB3, traffic drops will be observed due to multiple PFEs (Packet I blackholing traffic. This issue happens when an SFB3 comes up online after an ungraceful offline follow fabric Link errors.
<a href="#">1807410</a> Critical	SFB power off/unplug followed by ungraceful SPMB restart leads to SPMB crash Product-Group=junos Severity=Critical	On MX2020 and MX2010 platforms, during fabric link training, if the SFB (Switch Fabric Board) suddenly unplugged at a specific moment, a SPMB (Switch Processor Mezzanine Board) crash can be seen. It is a t
<a href="#">1812046</a> Minor	On MX2K, offline manually SFB2 or SFB3 or Plane to recover from a fabric link training failure, fabric manager is not able to turn off the fabric links on a neighbor slot FPC Product-Group=junos Severity=Minor	Once SFB2 or SFB3 or plane is manually offline in an attempt to recover from a Fabric Training Failure c be able to stop the high speed link and is ending up with training failure as well.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Multiprotocol Label Switching</b>
<a href="#">1773796</a>	The LSP name and bandwidth values	In "show mpls lsp autobandwidth name X" command when the name of the Link State Packet (LSP) is gre

Minor are displayed continuously in "show mpls lsp autobandwidth name X" command  
Product-Group=junos  
Severity=Minor

column with LSP name and the second column with the Last bandwidth are merged.

PR Number	Synopsis	Category: For multicast snooping on MX
<a href="#">1710565</a> Major	In a scaled setup mcsnoopd is taking high CPU causing traffic drop Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, whenever a commit is done, that involves mcsnoopd daemon creation/deletion, interface add/delete to VLAN, interface enable/disable, IGMP (Internet Group Mana (Multicast Listener Discovery) snooping related config commands) mcsnoopd will consume CPU. In less s VLANs and few hundred IGMP snooping memberships), the CPU time taken is less. In a more scaled setu and a few thousand IGMP snooping memberships), the CPU may reach >90%. Since mcsnoopd is taking h like rpd. It may affect all the protocols if the CPU is not available to the protocols/daemons. This can i traffic drop.
<a href="#">1711153</a> Major	A crash can be observed for 'mcsnoopd' process when the VLAN name for igmp-snooping has certain characters Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, a crash can be observed for the 'mcsnoopd' process. This issu VLAN (Virtual Local Area Network) style of igmp-snooping (internet group messaging protocol configurat and the VLAN name begins with the word all and has certain other characters. The workaround is not to
<a href="#">1758369</a> Minor	The mcsnoopd crash will be seen in MC-LAG configured scenario Product-Group=junos Severity=Minor	On all MX platforms, traffic drop will be seen due to mcsnoopd crash when MC-LAG (Multichassis Link Ag with selective ICL (Interchassis Link) feature configured.
PR Number	Synopsis	Category: Multicast for L3VPNs
<a href="#">1652481</a> Minor	MVPN Inter-AS option B shows updated PMSI attribute tunnel id when advertising type-3 routes to Intra-AS PE Product-Group=junos Severity=Minor	PMSI attribute should be changed when sending Multicast VPN auto-discovery(AD) route from one regio groups in Multicast VPN) or in case it is sent to External Border Gateway Protocol (EBGP) peer or from E (IBGP) peer. For IBGP to IBGP in case of RR (Route Reflector), ideally it should just reflect the route anc change in PMSI may result into traffic drop for internal RR clients.
<a href="#">1682573</a> Major	Core observed with multiple daemons restart Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms supporting dual-RE (Routing Engine) and NSR (Nonstop Active multiple daemons restart. There is no functional impact and the system recovers after the restart.
PR Number	Synopsis	Category: Jflow and sflow on MX
<a href="#">1604283</a> Minor	The adapted sample rate might get reset to the configured sample rate without changing the sampling rate information in sFlow datagrams Product-Group=junos Severity=Minor	On all MX platforms, when setting a new interface and enabling sFlow technology on a new interface is sampling rate might get reset but the flow samples might still show that the packets are sampled at the inconsistency between flow information and actual sample rate might cause issues on the collector side
PR Number	Synopsis	Category: MX Timing software
<a href="#">1601843</a> Major	PTP stateful configuration along with ordinary clock mode does not work together Product-Group=junos Severity=Major	When PTP is on default profile & PTPoE is configured in stateful with ordinary clock-mode configuration does not throw commit error. There are no error logs reported with below unsupported cc configuration: root@device# show protocols ptp clock-mode ordinary; stateful { interface xe-0/0/0.0 { i } } } } Stateful port configuration for PTP over Ethernet and default profile is supported only on bounda mode. Work around is to change the clock-mode or to remove stateful configuration.
PR Number	Synopsis	Category: MX104 Software - Timing
<a href="#">1782868</a> Major	MX104 AFEB might crash following a change of PTP clock source. Product-Group=junos Severity=Major	On MX104, the AFEB could crash and reboot following a change of PTP GM clock source, which affects t

PR Number	Synopsis	Category: MX10K platform
<a href="#">1684728</a> Major	An interface configured as 1G may flap on a port with the mixed speeds of 1G and 10G after a PIC restart Product-Group=junos Severity=Major	On MX10008, MX10004, and MX10016 platforms with LC2101, when the channelized interfaces of a port of 1G and 10G, after a Physical Interface Card (PIC) reboot the 1G channelized interface will keep flapping will impact all the services running through the 1G channelized interface.
PR Number	Synopsis	Category: Track Mt Rainier RE platform software issues
<a href="#">1782062</a> Minor	The interface fxp0 deactivation or activation is not captured due to improper date format Product-Group=junos Severity=Minor	On MX VMHost platforms, the interface fxp0 state is not captured since the script to bring up the interface date field.
PR Number	Synopsis	Category: Odin Timing software
<a href="#">1829340</a> Major	On Junos ACX710 Platforms the clksyncd error is seen affecting IPC Product-Group=junos Severity=Major	ACX710 Junos Platforms reports error clksyncd-service subsystem is not responding to management request commit causing clksyncd CLI to stuck affecting IPC (Interprocess communication).
PR Number	Synopsis	Category: OS IPv4/ARP/ICMPv4
<a href="#">1740873</a> Major	ARP resolution will not work properly if the L3 interfaces are configured with native vlan-id Product-Group=junos Severity=Major	On MX platforms with MPC10/MPC11/LC9600 linecards and MX304, in problematic scenario if a device in the packet goes out tagged and peer device receives tagged packet. If the peer device is not configured to different native VLAN configuration or no VLAN configuration), the peer will drop the packet. Due to resolution would fail which leads to traffic drop. Ideally if the L3 interfaces are configured with native-untagged.
PR Number	Synopsis	Category: FreeBSD Kernel Infrastructure
<a href="#">1838460</a> Major	Junos OS: A local attacker with shell access can execute arbitrary code (CVE-2025-21590) Product-Group=junos Severity=Major	An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks Junos OS privileges to compromise the integrity of the device. Please refer to <a href="https://supportportal.juniper.net/">https://supportportal.juniper.net/</a>
PR Number	Synopsis	Category: "ifstate" infrastructure
<a href="#">1484322</a> Major	The SNMP index in the Packet Forwarding Engine reports as 0, causing sFlow to report either IIF or OIF (not both) as 0 in the sFlow record data at the collector. Product-Group=junos Severity=Major	The SNMP index for bundle interface might become zero in PFE after restarting the FPC. This could cause "input interface value" (IIF) or "output interface value" (OIF) as 0 value.
PR Number	Synopsis	Category: Kernel MPLS / Tag / P2MP Infrastructure
<a href="#">1702220</a> Major	LDP flaps will be observed having LT interface with VLAN and LDP running between the logical-system instance and global instance Product-Group=junos Severity=Major	On Junos platforms, when the LT (Logical Tunnel) interface with VLAN and LDP (Label Distribution Protocol) system instance and global instance LDP flaps are observed.
PR Number	Synopsis	Category: IPv6/ND/ICMPv6 issues

<a href="#">1694009</a> Minor	NDP can't resolve neighbor after clearing IPv6 neighbor Product-Group=junos Severity=Minor	On all Junos platforms, when the user route is present with the same prefix (address) as ND (Neighbor I neighbors can delete the user route as well. Because of this, the RPD and forwarding state can go out o
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: JUNOS Network App Infrastructure (for ping, traceroute, etc)</b>
<a href="#">1717843</a> Critical	JUNOS - FILE COPY - Secure file copy using VRF succeeds even on disabling VRF Product-Group=junos Severity=Critical	
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: PFE Peer Infra</b>
<a href="#">1801535</a> Minor	CPU usage gets spiked for eventd due to flooding of pfe_khms_spurious_wakeup log Product-Group=junos Severity=Minor	On all Junos platforms, CPU usage gets spiked for eventd due to flooding of pfe_khms_spurious_wakeup printed under LOG_ERROR and flooded with default log level. This causes restart which will impact nor
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Kernel Tunnel Interface Infrastructure</b>
<a href="#">1760684</a> Minor	DNS proxy feature not working on logical tunnel interfaces Product-Group=junos Severity=Minor	DNS proxy feature does not process DNS queries that are received on logical tunnel interface
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: OSPF routing protocol</b>
<a href="#">1704521</a> Minor	On all Junos and Junos OS Evolved platforms, the TI-LFA and Legacy LFA are mutually exclusive, and the commit check will fail and blocks LFA on one instance Product-Group=junos Severity=Minor	On all Junos and Junos OS Evolved platforms, if configuring LFA (Loop-Free Alternate)/RLFA (Remote LF instance and TI-LFA (topology independent LFA) in the master instance, along with Segment Routing and convergence, the commit check fails and blocks LFA on one instance.
<a href="#">1827435</a> Major	OSPF LSA flooding is impacted after database recovers from 'ignore' state when 'database-protection' is triggered Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, when the LSA (Link State Advertisement) count exceeds tl 'database-protection' feature in OSPFV2 (Open Shortest Path First Version 2), the OSPF database (DB) er recovered, OSPF LSA flooding is stopped on some interfaces.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Express Paradise PFE Sflow</b>
<a href="#">1803542</a> Minor	PTX10008 - Recurring logs -ppcfpc-multi-svcs.elf: FDB :: lpv4 route operation 2 failed. Rt_index 1801 Product-Group=junos Severity=Minor	Recurring logs -ppcfpc-multi-svcs.elf: FDB :: lpv4 route operation 2 failed. Rt_index are seen in PTX100
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Phone-Home-Client Infrastructure</b>
<a href="#">1743222</a> Major	After ZTP process, the configuration fetch from the script path in event-options is impacted Product-Group=junos Severity=Major	On EX4300-MP platforms, when event-options are configured and ZTP (Zero Touch Provisioning) is perfor retrieved as the script path is not configured properly.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Protocol Independant Multicast</b>

<a href="#">1701189</a> Major	The mcsnoopd process crashes when snooping configurations are removed Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when snooping configurations are removed immediately after Graceful Restart), it crashes generating a crash file. This has an impact on layer 2 multicast traffic.
<a href="#">1767314</a> Major	RPD may restart unexpectedly when MSDP peers were reset or closed Product-Group=junos Severity=Major	When an MSDP peer is terminated, the peer's information may not be cleaned up properly. Causing the
<a href="#">1793598</a> Critical	Multicast Traffic loss (20s - 30s) is seen during the reconvergence after link flap Product-Group=junos Severity=Critical	On Junos and Junos Evolved platforms, When device is configured with MoFRR(Multicast-Only Fast Reroute Multicast) and also when the upstream links to the source of the multicast traffic flow is made down an around 20 to 30 seconds until the link comes up.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related to PKI daemon</b>
<a href="#">1646925</a> Major	While updating ca-profile-group certificates, all Junos and EVO platforms may face certificate load failure when a configuration commit is made in the background Product-Group=junos Severity=Major	All junos platforms using PKI services may face certificate load failure when a private commit or any key is made in the background. The certificates will need to be manually cleared first before attempting another load subsequent load requests will fail.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: vMX Platform Infrastructure related issue tracking</b>
<a href="#">1729152</a> Minor	The FPC crash or flap in protocols will be seen as soon as port-mirroring or firewall filters with syslog action is enabled Product-Group=junos Severity=Minor	On MX150 platform, when port-mirroring or firewall with syslog configuration is enabled, there will be a depletion of buffer memory which will lead to flap in the protocols or the (Flexible PIC Concentrators) I
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: VRR (Virtual Route Reflector) for MX</b>
<a href="#">1644806</a> Minor	The video console for vRR might not work after an upgrade to Junos with upgraded FreeBSD Product-Group=junos Severity=Minor	Video console (ttyv0) for vRR might not work when upgraded from legacy JUNOS [release 16.1 using FreeBSD [release 20.4 using FreeBSD 10 and later] and vRR is spawned with a video console. Post upgrade serial any issues but video console does not work. This happens because video console is not configured to be released.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Periodic Packet Management Daemon</b>
<a href="#">1813841</a> Major	Local repair does not happen if BFD is configured on MX platforms with MPC7E line card Product-Group=junos Severity=Major	On MX Series platforms with MPC7E line card, the BFD (Bidirectional Forwarding Detection) local repair does not move to the backup path causing traffic blackhole. This issue could be seen after any action that causes PFE (Packet Forwarding Engine) shutdown.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: PPPoE functional plugin for bbe-smgd</b>
<a href="#">1580812</a> Minor	The subscribers over PS interface are not cleared after FPC offline Product-Group=junos Severity=Minor	On all platforms where PS (Pseudowire Subscriber) interface is supported, the subscribers may not be cleared
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: N/A:sw-rio-timing</b>
<a href="#">1830382</a> Major	The PTP global info parameters announce-interval, synchronization-interval, and delay-response-interval	On the Junos ACX5448 platform, the PTP min and max announce, sync and delay-request/response do not show in the CLI output "show ptp global-information".

unicast packets are not captured as expected  
Product-Group=junos  
Severity=Major

PR Number	Synopsis	Category: Routing Information Protocol
<a href="#">1660424</a> Minor	A policy with a policy action "community" configuration may not work Product-Group=junos Severity=Minor	On all Junos and Evolved platforms, when a policy with policy action "community set/add/delete" is configured under Routing Information Protocol(RIP) protocol, community configuration may not work.
<a href="#">1726028</a> Major	Neighbor state is down while checking RIPng neighbor information Product-Group=junos Severity=Major	When a virtual IP is configured over an IRB interface, IFA having the virtual IP is considered by RIPng and discarded with the error (errno : Address already in use), which is causing RIPng neighbor state to be down.
PR Number	Synopsis	Category: RPD Interfaces related issues
<a href="#">1798801</a> Major	MPLS/RSVP LSP self-ping behaviour differs from expected behaviour causing self-ping time out Product-Group=junos Severity=Major	On Junos OS Platforms, configured with Multiprotocol Label Switching (MPLS)/Resource Reservation Protocol and firewall filter applied on the loopback with prefix list that does not include the interface address is observed.
PR Number	Synopsis	Category: KRT Queue issues within RPD
<a href="#">1749252</a> Major	The rpd process shuts down on all Junos and Junos OS Evolved platforms Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms with BGP flow specification configuration, the rpd process gets removed due to traffic churn and will result in traffic drop.
<a href="#">1761667</a> Major	The rpd process and chassisd process crash is seen Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms configuring BGP causes the rpd to crash abnormally and later crash is seen.
<a href="#">1831421</a> Critical	Multiple flaps on BGP routes causing traffic blackholing Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms, BGP (Border Gateway Protocol) route with PNH1 (Preserve Next Hop) is not correctly during rapid route fluctuations (e.g., link flaps). Specifically, when the preferred route (Rt1) is added, the system might incorrectly associate the PNH with an outdated route (Rt2).
PR Number	Synopsis	Category: RPD Next-hop issues including indirect, CNH, and MCNH
<a href="#">1583245</a> Major	The next hop of static LSP for MPLS might get stuck in dead state after changing the network mask of the outgoing interface Product-Group=junos Severity=Major	With static label-switched path (LSP) for MPLS configured with next hop and multiple interface address next hop might get stuck in dead state when changing the network mask and keeping the IP address unchanged through which the LSP next hop is reachable.
<a href="#">1698516</a> Critical	The mpls routing table resolving over IPv6 prefix causes traffic drop Product-Group=junos Severity=Critical	On all Junos MX/EX92xx platforms traffic drop is seen when mpls routing table is resolving over a IPv6 prefix.
<a href="#">1704714</a> Major	Incorrect reporting of element 47 of ipfix/jflow service Product-Group=junos Severity=Major	
<a href="#">1716436</a> Major	Traffic loss due to incorrect route resolution and KRT queue getting stuck	On all Junos and Junos OS Evolved platforms, due to a bug in route resolution over specific types of next hop and the nexthop chain keeps expanding. Due to this issue, the depth of recursion gets higher than supported.

with 'EINVAL -- Bad parameter in request' error  
Product-Group=junos  
Severity=Major

queue returns errors for nexthops. As a result, there will be incorrect route resolution, traffic loss and daemon) crashes. The necessary configurations and conditions that will result in this issue are below 1. Independent Convergence (PIC) ("protect core") is configured and BGP receives same prefix from EBGP ; Unicast) with "protection" to create backup path to protect the active and BGP receives same prefix from recursive Route resolvability situations like Resolving using Default-route (not having proper resolution

<a href="#">1777068</a> Minor	Policy Evaluation causing unrelated route flaps in Dynamic Tunnel setup Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms that support Dynamic tunnels, a policy evaluation of the route tunnel routes. The route flap for the tunnel route will cause traffic loss.
<a href="#">1808463</a> Major	CPU utilization of the rpd process stays high on all Junos and Junos OS Evolved platforms Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms in a corner case, the Routing Protocol Daemon (rpd) CPU utilization where recursive route resolution is involved. The rpd process will be continuously spinning in the re-resolution scheduling of other jobs and re-resolution of other routes impacting traffic.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: RPD policy options</b>
<a href="#">1714163</a> Critical	The static routes are installed in the routing table even though interface routes are not present Product-Group=junos Severity=Critical	On all Junos and Junos OS Evolved platforms, the static routes are installed in the routing table even though they are not present.
<a href="#">1849500</a> Major	Static route validation fails when using an interface-route leaked with rib-groups using "to rib " as matching condition under rib-groups import-policy Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, static route validation fails if it is using a leaked interface-route as matching condition under rib-groups import-policy. That would impact the traffic dependent on
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related route resolution routing infrastructure</b>
<a href="#">1737594</a> Critical	Traffic drop can be seen in the MPLS traffic Engineering scenario Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms, traffic drop can be seen in MPLS (Multi-Protocol Label Switching) (Interior Gateway Protocol Fast Reroute) and preserve next-hop hierarchy. This issue happens when the active route is withdrawn, while the above processing is done the session ID is associated with both the active route, the route gets deleted which triggers the IGP-FRR session ID to be down and the unicast (E) impact.
<a href="#">1818978</a> Major	The "preserve-nexthop-hierarchy" knob configured with VPLS , brings down the L3 protocol sessions running over the IRB interface Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, "preserve-nexthop-hierarchy" knob configured with Virtual Private Layer-3 (L3) control packets like that of Border Gateway Protocol (BGP) / Open Shortest Path First (OSPF) Bridging (IRB) interface to be dropped and brings down the protocol sessions.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: RPD route tables, resolver, routing instances, static routes</b>
<a href="#">1709741</a> Major	The rpd process crash on backup RE will be observed during configuration removal or restoration Product-Group=junos Severity=Major	The rpd process crash on backup RE will be observed during configuration removal or restoration.
<a href="#">1733803</a> Critical	IP-IP tunnel traffic drop is seen when "preserve-nexthop-hierarchy" knob is enabled Product-Group=junos Severity=Critical	On all MX and QFX platforms, in a specific scenario, when IP-in-IP tunnels are established between MX and QFX 'preserve-nexthop-hierarchy' configured on the MX device, the tunnel traffic drops on QFX (the receiving
<a href="#">1761191</a> Critical	Memory leak in rpd due to deactivation and activation of routing-instances, interfaces and protocols	On all Junos and Junos OS Evolved platforms with Border Gateway Protocol (BGP) rib-sharding enabled and configured, upon deactivation and activation of routing-instances, interfaces and protocols together, there will be no traffic impact at this time because memory leak is very slow.

Product-Group=junos  
Severity=Critical

<a href="#">1771344</a> Minor	Leaked routes via BGP rib-group remains in hidden state even though "loops" is configured with any value greater than one Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms having BGP (Border Gateway protocol) configured, when routing instance to another having the same AS (Autonomous System) number and one of the routing-instances, it is observed that even after configuring "loops" with any value greater than one as the number of hidden instead of being active which results in traffic drop.
<a href="#">1806694</a> Major	Junos OS and Junos OS Evolved: On SRV6 enabled devices, an attacker sending a malformed BGP update can cause the rpd to crash (CVE-2025-21593) Product-Group=junos Severity=Major	An Improper Control of a Resource Through its Lifetime vulnerability in the routing protocol daemon (rpd) on Junos OS Evolved allows an unauthenticated network-based attacker to cause a Denial-of-Service (DoS) <a href="https://supportportal.juniper.net/JSA92861">https://supportportal.juniper.net/JSA92861</a> for more information.
<a href="#">1807037</a> Minor	BGP backup routes are installed as primary routes after enabling 'protect core' feature Product-Group=junos Severity=Minor	On all Junos and Junos OS Evolved platforms when Border Gateway Protocol (BGP) multipath is enabled (L3VPN) routes and 'protect core' is enabled on the Virtual Routing and Forwarding (VRF) instance, the backup path. The Next hop weight value is not updated correctly, it is weight 0x1 instead of weight 0x4000 for
<a href="#">1812124</a> Minor	The rpd process crash is observed when the label received exceeds the configured maximum-labels 16 Product-Group=junos Severity=Minor	On Junos and Junos Evolved platforms, the rpd process crash is observed on both REs (Routing Engines) maximum-labels under MPLS(Multi Protocol Label System) address family is configured as 16 and an ext
<a href="#">1812844</a> Major	The rpd process crash is observed when policy condition is applied to the route with a next-hop interface having nonzero logical unit Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved Platforms configured with "policy-options condition if-route-exists active" will be observed when this policy is being applied to the route with a next-hop interface having nonzero configured under policy's address-family differs from the route's next-hop interface.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: show route table commands, tracing, and syslog facilities</b>
<a href="#">1812009</a> Major	The rpd process crash is observed when there are catastrophic changes under the particular routing instance configuration Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, when there is any catastrophic changes made in the configuration of a particular routing instance will lead to the rpd process crash.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Resource Reservation Protocol</b>
<a href="#">1587177</a> Major	Soft-preemption does not work after applying "subscription 0" configuration on RSVP interfaces Product-Group=junos Severity=Major	On the transit label-switching router (LSR), if soft-preemption is configured under both RSVP and label-switched-path (LSP), "preemption aggressive" is configured under RSVP, the soft-preemption does not work for some LSPs after a change on all RSVP interfaces.
<a href="#">1694777</a> Major	Restarting FPC or router reboot might causes some CCC interfaces to go down due to a 'Remote CCC down' Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, if CCC (Circuit Cross-Connect) is configured to use a label-switched-path (LSP) and no strict ERO (Explicit Route Object) configuration, then restarting egress CCC node or rest containing remote-interface-switch configuration multiple times may cause CCC to remain stuck in remote-interface-switch configuration. (The knob 'remote-interface-switch' is configured on the egress LER of the RSVP-TE LSP (Resource Reservation Protocol Engineering label-switched-path) which binds the LSP terminating on the node to a local interface).
<a href="#">1723229</a> Minor	The rpd process crash is observed when RSVP LSP at Juniper transit/ingress router receives RESV message with RESVCONF object in multi vendor deployment Product-Group=junos Severity=Minor	On all Junos and Junos OS Evolved platforms (For QFX5100, only in Virtual Chassis-VC setup) with RSVP (Label-Switched Path) configured in multi vendor deployment and Juniper router is acting as a transit/ingress router, if a Request message is received with RESVCONF object from other vendors, rpd process crash will be observed.

<a href="#">1732862</a> Major	Junos OS and Junos OS Evolved: Memory leak due to RSVP neighbor persistent error leading to kernel crash (CVE-2024-39560) Product-Group=junos Severity=Major	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Junos OS Evolved allows a logically adjacent downstream RSVP neighbor to cause kernel memory exhaustion, leading to Denial of Service (DoS). Please refer to <a href="https://supportportal.juniper.net/JSA83020">https://supportportal.juniper.net/JSA83020</a> for more information.
<a href="#">1800034</a> Major	Traffic drop observed after graceful restart event Product-Group=junos Severity=Major	If a link along the path of a Label Switched Path (LSP) flaps briefly such that the router at upstream end goes down but only the router at the downstream end does, then the upstream router does not send a ResvTear message, that should be taken after next-hop link down. This will result in longer than expected traffic loss at the downstream end of the flapping link.
<a href="#">1820893</a> Major	The detour path is not coming up when the detour hop limit is set to 255 Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms configured with MPLS/RSVP (Multiprotocol Label Switching/RSVP) path might not form when the "fast-reroute hop-limit" is set to 255. Thus, traffic loss will be observed and detour will not happen.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: RPD API infrastructure</b>
<a href="#">1710274</a> Critical	Next Hop counts are not as expected Product-Group=junos Severity=Critical	Next Hop counts are not as expected
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: RPM and TWAMP</b>
<a href="#">1651489</a> Minor	RPM probes configured with target HTTP/HTTPS URLs will fail if the URL contains '[' or ']' Product-Group=junos Severity=Minor	On all Junos-based platforms starting with 21.4 releases, if RPM (Real-time Performance Monitoring) probes configured with HTTP/HTTPS (HyperText Transfer Protocol/Secure) URL (Universal Resource Locator) that comes with option will fail with an error: "Unable to resolve target name".
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Scuba chassis software</b>
<a href="#">1743686</a> Minor	Due to SPMB restarts in the middle of the FPC boot process, FPC won't come up Product-Group=junos Severity=Minor	On MX2010 or MX2020 platforms, SPMB restarts during the FPCs boot process will cause some FPCs to be in a non-operational state.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Scuba fabric software</b>
<a href="#">1807812</a> Critical	MX platforms with some MPCs could run into cm_error during ungraceful SIB or Peer-FPC power off event or due to bad fabric links Product-Group=junos Severity=Critical	During ungraceful Peer-SFB/Peer-FPC offline or due to a bad fabric link XM ASIC based FPCs can hit CPQ queue resulting in PFE Disable action. This PR fixes the underlying reason for the CPQ Underrun error on MX platforms.
<a href="#">1811474</a> Major	In Junos MX platforms specifically MX2010 and MX2020 with SFB2 Fabric installed replacing MPC9E linecards with MPC6E linecards results in all SFB2 fabric get into check state and FPCs become destination error and offline Product-Group=junos Severity=Major	On Junos MX platforms specifically MX2010 and MX2020 with SFB2 (Switch Fabric Board) Fabric installed MPC6E in slot (swapping specifically with MPC9E linecard), fabric get into check state and all FPCs go offline. Due to this, traffic loss can occur.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: HA functionality on ASP</b>
<a href="#">1853304</a> Major	Traffic was lost on MX platforms following a Routing Engine failover Product-Group=junos Severity=Major	On Junos MX240/MX480/MX960/MX2010/MX2020 platforms which support TLB (Traffic-Load Balancer) traffic is not properly synchronized with the new master RE (Routing Engine) after a RE failover causing traffic loss.

PR Number	Synopsis	Category: SNMP Infrastructure (snmpd, mib2d)
<a href="#">1734549</a> Minor	Syslog messages modification for SNMPv3 authentication failure Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, the syslog message for a wrong auth/privacy and password hash information.
PR Number	Synopsis	Category: Generic platform and infra issues for MS-MIC and MS-MPC(XLP)
<a href="#">1750823</a> Minor	The mspmand daemon crashes causing traffic loss Product-Group=junos Severity=Minor	On Junos platforms with MS-MPC (Multiservices Modular Port Concentrator) like MX240, MX480, MX960, the mspmand daemon (Multiservices PIC Manager Daemon) crash can be observed which causes traffic loss.
<a href="#">1766347</a> Minor	BGP protocol flap observed due to unsupported configuration of TCP-MSS or MTU on the service-interfaces Product-Group=junos Severity=Minor	On MX platforms with service cards like MSMPC/SPC3, BGP protocol flaps due to TCP-MSS or MTU config (ms/vms/ams). This is an unsupported configuration and should not be configured.
PR Number	Synopsis	Category: SFW, CGNAT on MS-MIC/MS-MPC (XLP)
<a href="#">1783745</a> Major	The mspmand process might crash on the MS-MPC during deletion of service-sets configuration Product-Group=junos Severity=Major	On Junos MX platforms with MS-MPC(Multiservices Modular Port Concentrator) line cards, with Network Block Allocation) enabled, multiple times deletion of service-sets configuration, will lead to PFE (Packet Forwarding Engine) crash which mspmand cores and MPC goes offline and during this interval, there is a drop in traffic.
<a href="#">1826847</a> Minor	Large number of CGNAT NAT pool out-of-address errors and stale NAT mappings for SIP traffic are observed Product-Group=junos Severity=Minor	On MX platforms with MS-MPC and CGNAT (Carrier-Grade Network Address Translation) configured, a large number of stale NAT mappings for SIP (Session Initiation Protocol) traffic can occur. This can lead to a lack of available connections to be dropped.
PR Number	Synopsis	Category: SRX Argon module
<a href="#">1661766</a> Major	Junos OS: SRX Series: A large amount of traffic being processed by ATP Cloud can lead to a PFE crash (CVE-2024-47506) Product-Group=junos Severity=Major	A Deadlock vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on SRX Series devices allows an attacker to cause a Denial of Service (DoS). Please refer to <a href="https://supportportal.juniper.net/JS92860">https://supportportal.juniper.net/JS92860</a> for more information.
<a href="#">1801893</a> Critical	Junos OS: SRX Series: Low privileged user able to access highly sensitive information on file system (CVE-2025-21592) Product-Group=junos Severity=Critical	An Exposure of Sensitive Information to an Unauthorized Actor vulnerability in the command-line interface on SRX Series devices allows a local, low-privileged user with access to the Junos CLI to view the contents of files on the file system. Please refer to <a href="https://supportportal.juniper.net/JSA92860">https://supportportal.juniper.net/JSA92860</a> for more information.
<a href="#">1828721</a> Minor	Flowd crash seen on SRX platforms with security metadata streaming enabled and then enabling AAMW traceoptions Product-Group=junos Severity=Minor	On all SRX platforms, when security metadata streaming is configured, the flowd process crashes if you enable AAMW traceoptions and traffic and service.
PR Number	Synopsis	Category: SRX branch platforms
<a href="#">1783757</a> Major	Junos OS: SRX Series, QFX Series, MX Series and EX Series: Receiving specific HTTPS traffic causes resource	An Uncontrolled Resource Consumption vulnerability in the http daemon (httpd) of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to cause Denial-of-Service (DoS). Please refer to <a href="https://supportportal.juniper.net/JSA88124">https://supportportal.juniper.net/JSA88124</a> for more information.

	exhaustion (CVE-2024-47497) Product-Group=junos Severity=Major	
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Stout card (MPC7) fabric issues</b>
<a href="#">1766578</a> Minor	The FPC Crash will be observed on Junos MX platforms Product-Group=junos Severity=Minor	On Junos MX platforms with dual RE, repeated reboots of a SCBE2/ SCBE3 (Switch Control Board) during multiple PCIe (Peripheral Component Interconnect) interface error alarms. This results in input/output ( SCBE2/ SCBE3), leading them to enter a faulty state. Consequently, the affected FPC crashes, impacti
<a href="#">1768592</a> Major	The SFB3 will go offline during during SFB3 <-> ADC <-> MPC7E link initialization Product-Group=junos Severity=Major	On MX2020 and MX2010 platforms with Switch Fabric Boards (SFB) 3 and Modular Port Concentrators (M inserted via Adapter Card (ADC) MX2000-LC, SFB3 will go offline during SFB3 <-> ADC <-> MPC7E link ini timing issue and will not be seen with every SFB3 <-> ADC <-> MPC7E link initialization. It happens beca events occurring during MPC initialization.
<a href="#">1769983</a> Critical	At MX2020 with SFB3 and MPC7+ADC in FPC slot 11, link errors in fabric planes 1, 4, 7, 10 will be seen upon MPC7/ADC restart in FPC slot 11 Product-Group=junos Severity=Critical	On the Junos MX2020 with SFB3 and MPC7+ADC in FPC slot 11, link errors in fabric planes 1, 4, 7, and 10 FPC slot 11. The link errors will come along with the 'failed word alignment' syslog message logged by h scenario, the traffic impact will be observed as some of the fabric links do not come online.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: MPC7E, MPC8E and MPC9E timing and synchronization</b>
<a href="#">1806526</a> Major	Chassis not recovering clock from GM, but still advertisement of GM provided clock-class to downstream node Product-Group=junos Severity=Major	On Junos MX platforms, PLL gets frozen because of the Hardware failure but still advertises the GM pro synchronization failure and potential service impact. This affects clock signals distributed to all devices degradation. The issue affects line-cards from MPC3E to MPC10E, chassis with SCBE3, and platforms suc
<a href="#">1830281</a> Major	Sourceport-ID comparison resulting in higher value for MPC7E compared to MPC5E for distributed PTP architecture Product-Group=junos Severity=Major	SourcePort-ID comparison across line cards between MPC7E and MPC5E/6E/3E-NG/2E-NG shall result in compared to MPC7E/8E/9E/10E.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: MX10002 Platform SW - Platform s/w defects</b>
<a href="#">1755585</a> Minor	VMHost memory exhaustion results in image installation failure and brings down the RE during the upgrade Product-Group=junos Severity=Minor	On VM Host platforms, if the available memory is lower than 7.5G, the VM Host software install fails an regarding the lack of space. If a reboot is followed after such failed installation, the RE (Routing Engine disk.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: MX10002 Platform SW - Platform s/w defects</b>
<a href="#">1809306</a> Minor	On Junos MX204 platform and platforms with MPC7E/8E/9E, JNP10K-LC2101, JNP10003-LC2103, JNP10K-LC480 line cards, the interface goes down when re-initialisation issue occurs, causing 'Avago SERDES' EA (Eagle ASIC) chip crash Product-Group=junos Severity=Minor	On Junos MX204 platform and platforms with MPC7E/8E/9E, JNP10K-LC2101, JNP10003-LC2103, JNP10K down when re-initialisation issue occurs as part of system reboot, FPC(Flexible PIC Concentrators) resta causing 'Avago SERDES' EA (Eagle ASIC) chip crash.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related to broadband edge apps (PPP, DHCP) on ZT/YT</b>
<a href="#">1755036</a> Major	Incorrect COS configuration installation on pfe caused by high line card CPU Product-Group=junos Severity=Major	On Junos platforms with line cards like MPC10, MPC11, LC9600 and MX304 platforms, incorrect COS con in wrong traffic forwarding or traffic loss due to line card CPU getting hung.

<a href="#">1784914</a> Minor	The backup routing-engine mac address is not resolved on Junos MX platforms with subscriber management configuration Product-Group=junos Severity=Minor	On Junos MX platforms with MPC 3NG, MPC5, MPC7 line cards with subscriber management configuration 18.4 release or higher, the backup routing-engine (REs) mac address does not get resolved during Flexib when the backup RE and the FPC reboot at the same time.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: ZT/YT pfe infra issues</b>
<a href="#">1674605</a> Minor	The unexpected error logs are observed on platforms with MPC10E or later line cards Product-Group=junos Severity=Minor	On platforms with MPC10E or later line cards, the unexpected error logs are observed, for remote inter
<a href="#">1684371</a> Major	MPC linecard memory leak Product-Group=junos Severity=Major	Due to a software bug that missing null check while coalescing of memory block, customer can observe either block the PPPoE/DHCP/L2TP subscribers login, or cause the FPC core dump.
<a href="#">1796344</a> Minor	PacketIO PFE process will drop small fragments of TCP and UDP packets destined to the routing engine Product-Group=junos Severity=Minor	On platforms running PacketIO PFE process (MPC10E, MPC11E, MX10K-LC9600, MX304 and all Junos OS E TCP and UDP packets destined to the routing engine will be dropped.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: ZT/YT pfe qos software issues</b>
<a href="#">1690818</a> Major	CoS rewrite rules will not be working on the IRB interface in Enhanced convergence mode Product-Group=junos Severity=Major	On all Junos MX platforms, if the class-of-service(CoS) rewrite rules are configured over the Integrated Enhanced convergence mode, the packets will not be overwritten as per the rewrite rules, and forward impacted.
<a href="#">1793375</a> Critical	CMErrors are observed on MX platforms running MPC10/MPC11 causing the PFE to be disabled Product-Group=junos Severity=Critical	On all MX platforms having MPC10 or MPC11 having class-of-service configured, it is observed that in a Logical)), when queues are oversubscribed and the output interface starts to get congested, "CMERROR "XQSS_CMERROR_SCHED_QL4_INT_REG_DQU_QSUM_UDR" error message is seen. These cm errors would disable or the action configured in the device.
<a href="#">1805343</a> Major	Host loopback wedge observed when oversubscribing queues and flapping subscribers Product-Group=junos Severity=Major	On Junos MX-Series using MPC10, MPC11, LC9600 line cards, host loopback wedge can be observed in a subscribers are flapping and class of service queues are over-subscribed. This can lead to a FPC (Flexibl impact traffic.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: ZT/YT pfe firewall software</b>
<a href="#">1736965</a> Minor	PFE wedge observed due to fast-lookup-filter change from <256 terms to >256 terms in the filter Product-Group=junos Severity=Minor	On MX platforms with MPC10, MPC11 and LC9600 cards and MC304 platform, firewall filters marked with cannot be added in excess of 256 in the existing filter. This causes PFE (Packet Forwarding Engine) wed
<a href="#">1775551</a> Minor	The error messages are observed on MX platforms for ICMP packets Product-Group=junos Severity=Minor	The MPC10 reporting error messages; afdt-trio: [Error] DFVCOMMON Packet buffer doesn't have sufficie Packet buffer size:2 Src and dst ports size:4
<a href="#">1802341</a> Major	Filter will be configured with incorrect vlan-IDs and commit error will not be displayed Product-Group=junos Severity=Major	On mx10008 platform, filter will be configured with incorrect vlan-IDs and commit error will not be displayed range of 0-4095 which is syntactically incorrect.
<a href="#">1802362</a>	Filter will be configured with incorrect	On MX10008 platforms, filter will be configured with incorrect vlan-IDs and commit error will not be displayed

Major	vlan-IDs and commit error will not be displayed Product-Group=junos Severity=Major	range of 0-4095 which is syntactically incorrect.
<a href="#">1808821</a> Minor	Traffic drop will be observed if bandwidth-percent policer action applied on an interface Product-Group=junos Severity=Minor	On all MX platforms with MPC10, MPC11, LC9600 and MX304, all traffic on an interface drops if it is host (PFE) with a PFE number other than 0 and 'family any' filter with bandwidth-percent policer action is ap
<a href="#">1840815</a> Major	[MX304] L2 policer may not work after rebooting chassis or fpc. Product-Group=junos Severity=Major	After rebooting chassis or fpc, L2 policer may not work sometimes due to not reflecting configuration p
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: ZT/YTpfe bridging, learning, stp, oam, irb software</b>
<a href="#">1766694</a> Minor	802.1p priority is preserved when traffic is sent from AFT with irb Product-Group=junos Severity=Minor	In AFT with IRB config, post the mpls decapsulation, irb egress processing is done which adds an L2enca preserved are also copied.
<a href="#">1850604</a> Major	Packet duplication and flooding issues are seen when vpls bridge domain is configured on an aggregated Ethernet and label-switched interface across multiple line cards Product-Group=junos Severity=Major	On MX240/MX480/MX960/MX2008/MX2010/MX2020/MX10003/MX10008/MX10016/MX10004 platforms wit bridge domain configured, when the core facing ecmp (Equal cost multipath) are across multiple line ca limit, packet flooding might be seen continuously for 5 mins after uplink or downlink going down causin
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: ZT/YT pfe I3 forwarding issues</b>
<a href="#">1759590</a> Minor	The aftd process crashes on MX304 continuously when turning up BGP neighbours with no LMIC card on slot 0 Product-Group=junos Severity=Minor	On MX304 platforms, when the slots 0 is empty or the LMIC card on slot 0 is inactive (PFE0 is inactive) a the aftd process crashes continuously when BGP neighbours are turned up. This leads to complete loss c
<a href="#">1774127</a> Major	Memory leak for deactivation/activation of SCU Product-Group=junos Severity=Major	On MX platforms with MPC10, MPC11, LC9600, and MX304-LMIC16, the heap memory leaks every time tf removed i.e. removed and re-applied resulting in restart of the line card. Heap leak is proportional to t being removed by related policy.
<a href="#">1776783</a> Minor	BGP session on MPLSoUDP tunnel will not be established Product-Group=junos Severity=Minor	On MX platforms with MPC1-MPC9/LC2103/LC2101/LC480 line cards and EX9200 platforms, Border Gate Multiprotocol Label Switching over User Datagram Protocol (MPLSoUDP) tunnel will not be established a doesn't carry IIF information.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Trio LU, IX, QX, MQ chip drivers, ucode &amp; related SW</b>
<a href="#">1733630</a> Major	Synopsis:JDI-RCT:M/Mx:Observed traps and erros @trap_ordinal_count: 1 Async XTXN Error PPE/Context 10/2 @ PC 0x71f3: cmd_fetch_add during self ISSU Product-Group=junos Severity=Major	During ISSU it is possible that ctrl-plane initiated counter operations might trigger a trap and be interpr
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related to broadband edge apps (PPP, DHCP) on Trio ch</b>
<a href="#">1649067</a> Minor	FPC might crash when the command "show vbf pseudo" executed Product-Group=junos	On all MX platforms running on the non-AFT line cards with subscriber management scenario, an FPC cr pfe debug command ?show vbf pseudo?. This happens when the AE member link on FPC is removed, anc command is executed on the PFE shell during a certain time window. The time window corresponds to a

	Severity=Minor	interface are in the state of being deleted which affects the traffic and result in routing re-distribution
<a href="#">1665234</a> Minor	The rpf-check feature might not be working in a Junos Subscriber management scenario Product-Group=junos Severity=Minor	On MX platforms installed with MPC linecard( except MPC10 onwards) and Subscriber management, if the routing-services as well as the reverse-path forwarding (RPF) check, the rpf-check feature might not be
<a href="#">1703910</a> Minor	The line card abruptly reboots when ISSU is performed Product-Group=junos Severity=Minor	On platforms supporting MPC3E/MPC4E/T4000-FPC5/EX9200-4QS/EX9200-2C-8XS/EX9200-MPC/EX9200-3 the line card abruptly rebooted with a process crash when ISSU (In-Service Software Upgrade) is performed
<a href="#">1747009</a> Major	Traffic from subscribers will be dropped by Junos based MX platforms Product-Group=junos Severity=Major	On Junos based MX platforms in enhanced subscriber management scenario, with 'routing-services' and ' from subscribers will be dropped.
<a href="#">1747205</a> Minor	FPC crash will be observed during login and logout of the subscribers Product-Group=junos Severity=Minor	On all MX platforms with a scaled number of more than 21k subscribers, during login and logout of the subscribers after which subscribers will not come up.
<a href="#">1773148</a> Minor	The demux0 interfaces won't show any data traffic (measured in packets per second) after the FPC restarts Product-Group=junos Severity=Minor	On MX platform, If the line card restarts while subscribers are still connected, there might be a delay in member interface back online. This delay can cause inaccurate updates to the demux interface information showing zero data traffic (measured in pps) even though there might actually be traffic flowing.
<a href="#">1788669</a> Minor	Traffic drop due to mac-validate failure on MX platforms Product-Group=junos Severity=Minor	On Junos MX platforms, when subscriber management is enabled and mac-validate is configured on interfaces attempting to add a new link to an existing AE (Aggregate Ethernet) bundle from a different FPC.
<a href="#">1846055</a> Critical	PPE traps and traffic wedges are seen when subscribers are forwarded through Soft-GRE tunnel Product-Group=junos Severity=Critical	On all Junos MX platforms with MPC2-9 linecards, when subscribers are forwarded through the Soft-GRE memory corruption occurs resulting in PPE (Packet Processing Engines) traps being generated and traffic
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Trio pfe qos software</b>
<a href="#">1687642</a> Minor	CoS memory errors are seen when "chassis traffic-manager enhanced-priority-mode" is configured Product-Group=junos Severity=Minor	On MX platforms, when "chassis traffic-manager enhanced-priority-mode" is configured, Class of Service The initial error "Uninitialized Memory" has no impact, but in a rare case with a subscriber high scale, CoS report COS_HALP allocation errors which would require an FPC reboot.
<a href="#">1736890</a> Minor	The CoS rewrite rules will not be working in the EVPN with IRB scenario Product-Group=junos Severity=Minor	On Junos platforms, the Class of Service(CoS) rewrite rules are not working in Ethernet Virtual Private Network and bridging (IRB) scenarios. The packets will not be overwritten as per the rewrite rules and traffic forwarding will not be working as expected.
<a href="#">1749775</a> Major	Shaping not working for the L2 PS interface with HQoS configured in the PWHT environment Product-Group=junos Severity=Major	On all MX platforms (except with line cards MPC10E, MPC11E, LC9600) in the PWHT (Pseudowire Header HQoS (Hierarchical Class-of-Service) is configured for the L2 (Layer 2) PS (Pseudowire Subscriber) interface encapsulation, shaping will not work for the L2 PS interface i.e. might result in traffic congestion and the L2 PS Service interface is not classified under the PS Transport interface queue instead gets into the
<a href="#">1772826</a> Major	Cos queueing issue with tunnel interface when HCOS hierarchy is configured on it Product-Group=junos Severity=Major	On Trio based Junos platforms, with Hierarchical class of service (HCoS) 2 level hierarchy configuration forwarding pipeline for Logical Tunnel IFLs was not having the right queue information leading to the packets leads to increased in usemeter numbers causing the FPC get into Major error. Logical tunnel IFLs will not
<a href="#">1783261</a> Minor	Parity error Alarm in Queueing Packet Reader block needs to be moved from severity Major to Minor	On all MX platforms with MPC7E/MPC8E/MPC9E/MPC10E/MPC11E/MPC12E/MPC13E/MX10K-LC2101/JNP-LC2103 , alarms "EA_PR_PROTECT_FSET_1_REG_DETECTED_SHAPE_RAM", "XQSS_CMERROR_PR_PROTECT_FSET_1_REG_DETECTED_CD" and "XQSS_CMERROR_PR_PROTECT_FSET_1_REG_DETECTED_CD"

Product-Group=junos  
Severity=Minor

Major, which in return invokes 'disable-pfe' action, if configured, which causes ports to go down on the

PR Number	Synopsis	Category: Trio pfe stateless firewall software
<a href="#">1573350</a> Minor	Traffic drop seen and filter not hitting as expected for match condition traffic class with FLT option configured Product-Group=junos Severity=Minor	On MX platform, when the "FLT(fast-lookup-filter)" statement is configured with a match that is not supported on hardware, traffic might be lost.
<a href="#">1680849</a> Major	The FPC crashes when "show filter memory" command is used during a firewall filter configuration change Product-Group=junos Severity=Major	On all Junos platforms, the FPC will crash when a firewall filter change is in progress and at the same time
<a href="#">1738672</a> Minor	FPC crashes due to back-to-back GRES Product-Group=junos Severity=Minor	On line cards such as MPC5E/MPC7E/LC480/MPC10E/11E/LC9600 and MX304 platforms, when multiple times (GRES) is performed, all the FPCs crashed.
<a href="#">1751494</a> Minor	Traffic loss observed when using ingress-queueing-filter on non zero PFE interface Product-Group=junos Severity=Minor	On MX series routers which support MPCs (Modular Port Concentrators), the ingress-queue-filter was not working. The issue is seen only on non zero PFE (Packet Forwarding Engine) interface.
<a href="#">1800623</a> Major	Wedge condition is seen on MX platforms with MPC10/MPC11/JNP10K-LC9600 and MX304 platform switch port utilization is above 80% Product-Group=junos Severity=Major	On MX platforms with MPC10/MPC11/JNP10K-LC9600 and MX304 platforms, if the switch port utilization is above 80% and any firewall filter that is configured with log/syslog firewall action on it, leading to the wedge condition, the PFE process to crash.
<a href="#">1827439</a> Major	A BFD flap and subsequent impact in the traffic is seen when BGP FlowSpec session goes down or withdrawal of all BGP FlowSpec routes making entries on netflow.0 table to zero at once Product-Group=junos Severity=Major	On MX platforms with ukern based line cards (till MPC9), when the BGP FlowSpec session goes down or withdrawal of all BGP FlowSpec routes making entries on netflow.0 table to zero at once, a BFD (Bidirectional Forwarding Detection) flap occurs.
PR Number	Synopsis	Category: Trio pfe bridging, learning, stp, oam, irb software
<a href="#">1742701</a> Major	Host-outbound traffic and certain transit traffic affected due to IRB/VRF to VPLS stitching scenario Product-Group=junos Severity=Major	On Junos MX204/MX240/MX480/MX960/MX2008/MX2010/MX2020/MX10003/MX10004/MX10008/MX100016/EX9200 platforms with MPC5E/MPC7E/MPC8E/MPC9E/MX10K-LC2101/JNP10K-LC2101/MX10K-LC2103/JNP10K-LC40XS/EX9200-12QS/EX9253-6Q12C/EX9253-6Q12C-M line cards, in an L3 Virtual Routing and Forwarding (VPLS) stitching scenario, where VPLS over BGP labeled unicast (BGP-LU) is configured and, due to VPLS loss for host-outbound traffic and certain transit traffic too.
<a href="#">1814521</a> Major	Traffic drop is observed after any add/change/delete event on IRB interfaces inside a VPLS deployment Product-Group=junos Severity=Major	On MX platforms using MPC3/5/7/9 line cards, traffic drops is seen after any add/change/delete of next-hop between different VLANs (Virtual Local Area Network) in a VPLS (Virtual Private LAN Service) deployment.
PR Number	Synopsis	Category: Trio pfe l3 forwarding issues
<a href="#">1751699</a> Critical	Traffic loss with preserve-nexthop-hierarchy enabled on MX platforms with a combination of MPC1-9, LC480, LC2101, and MPC10E, MPC11E, LC9600 line cards Product-Group=junos Severity=Critical	On MX platform with a combination of MPC1-9, LC480, LC2101, and MPC10E, MPC11E, LC9600 line cards enabled and maximum-ecmp configured with more than 16 next-hops in the MPLS FRR (Multiprotocol Label Switching) Multipath scenario, packet loss during PFE local repair on the interface or session on MX platform with MPC1-9, LC480, LC2101 line cards only, OR with MPC10E, MPC11E, LC9600 line cards, is proportional to the value in maximum-ecmp configuration.

<a href="#">1763890</a> Major	ISIS adjacency failed to be up if gr-interface and underlay interface on same pfe instance Product-Group=junos Severity=Major	When gr and wan interface are on same pfe, when the ISISoGRE packet is received, l2 header doesnt get dropping the packet. As a result ISISoGRE doesnt come up. When the interfaces are on different pfe, w/ PFE is L3 payload and eventually it works.
<a href="#">1784593</a> Major	Junos OS: MX Series: The PFE will crash on running specific command (CVE-2024-47496) Product-Group=junos Severity=Major	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an attacker to cause a Denial-of-Service (DoS). Please refer to <a href="https://supportportal.juniper.net/JSA88123">https://supportportal.juniper.net/JSA88123</a>
<a href="#">1841876</a> Major	Q-in-Q transit traffic will be lost when Tag Protocol ID (TPID) is different than 0x8100 Product-Group=junos Severity=Major	In different MX series routers references, when Q-in-Q is configured with outer Vlan Tag protocol ID (TPID) lost and will not find its destination.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: DDos Support on MX</b>
<a href="#">1733477</a> Minor	Harmless logs "DDOS : Failed to insert flow to lkup map for proto: 3c00" observed in syslog Product-Group=junos Severity=Minor	"Failed to insert flow to lkup map for proto: 3c00" messages reported repeatedly in the syslog/message: database
<a href="#">1807538</a> Major	DDOS related Error messages can be seen on MX platforms Product-Group=junos Severity=Major	On certain Junos MX platforms with SCFD (Suspicious Control Flow Detection) enabled, error messages related to SCFD (Suspicious Control Flow Detection) protection can be seen when traffic volume is high with varied flows. There is no service impact observed.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Authentication, Authorization, Accounting, PAM (RADIUS/tacplus)</b>
<a href="#">1802329</a> Major	Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596) Product-Group=junos Severity=Major	An Authentication Bypass by Spoofing vulnerability in the RADIUS protocol of Juniper Networks Junos OS allows an on-path attacker between a RADIUS server and a RADIUS client to bypass authentication when RADIUS accounting is enabled. Please refer to <a href="https://supportportal.juniper.net/JSA88210">https://supportportal.juniper.net/JSA88210</a> for more information.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Configuration mgmt, ffp, load-action, commit processing</b>
<a href="#">1818692</a> Major	Configuration commit fails due to mustd process crash Product-Group=junos Severity=Major	Core dumps in mustd seen committing a change to a large prefix-list used by BGP
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: UI Infrastructure - mgd, DAX API, DDL/ODL</b>
<a href="#">1636085</a> Major	MTU configuration on an interface is not set as expected Product-Group=junos Severity=Major	On all Junos with persist-groups disabled ( on Junos persist-groups feature is enabled by default 19.4 or persist groups can be disabled (21.4R1 onwards persist-groups cannot be disabled on EVO) this issue can be reproduced during configuration expansion (when persist-groups is disabled) and a configuration is applied( for example, a configuration in which MTU is inherited from a groups configuration).
<a href="#">1645119</a> Critical	Junos OS and Junos OS Evolved: Confidential information in logs can be accessed by another user (CVE-2024-39532) Product-Group=junos Severity=Critical	An Insertion of Sensitive Information into Log File vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an attacker with high privileges to access sensitive information. Please refer to <a href="https://supportportal.juniper.net/JSA88210">https://supportportal.juniper.net/JSA88210</a>
<a href="#">1671038</a> Minor	Config failure can be seen after upgrade when modifying group for lsp auto-bandwidth Product-Group=junos	On all Junos and Junos EVO platforms, Config error is seen while modifying group for LSP auto-bandwidth

Severity=Minor

<a href="#">1784818</a> Major	The non-root user will not be able to copy files Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when logged in as a non-root user and trying to copy a file fr become non-root username although logged in as a non-root user and an error message is thrown.
<a href="#">1799277</a> Minor	The mgd crash is seen on aggregation device and upgrade is halted during upgrade to aggregated satellite switches Product-Group=junos Severity=Minor	The satellite package is not conforming to the expected junos version format leading to the problem re version string has been modified to handle such format incompatibility gracefully.
<a href="#">1825728</a> Minor	The mgd process crashes while using an FQDN in conjunction with the ephemeral configuration database Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, the mgd process crashes when device has an ephemeral conf (Fully Qualified Domain Name) is used for NTP (Network Time Protocol), radius-server, tacplus-server, e configuration or the ephemeral configuration database.
<a href="#">1847834</a> Major	Multiple daemons crash upon ephemeral or static db commits Product-Group=junos Severity=Major	On all Junos platforms with ephemeral configuration, multiple daemons like chassisd, dcd, l2ald, l2cpd ephemeral or static db commits causing service traffic impact. The services will self recover after the i
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related to Logging/Tracing, errmsg, eventd infrastruc</b>
<a href="#">1602536</a> Major	Observed memory leak in eventd leak during GRES Product-Group=junos Severity=Major	A minor memory leak is seen in the event-daemon process when multiple GRES switchovers are perform
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related to NETCONF</b>
<a href="#">1792362</a> Major	RPC request for file copy with routing instances is failing Product-Group=junos Severity=Major	On Junos OS and Junos OS Evolved platforms configured with routing instances, RPC (Remote Procedure instance fails. There is no service/traffic impact due to this issue.
<a href="#">1796297</a> Major	Error message not prompted on commit confirmed RPC sent in private mode on all Junos and Junos Evolved platforms Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, commit confirmed command executed with remote procedur mode is being allowed where ideally it should not be.
<a href="#">1800859</a> Minor	Configuration push to device using RPC resulted in incorrect policy order Product-Group=junos Severity=Minor	On all Junos and Junos OS Evolved platforms, RPC command with default-operation replace uses load u Junos 21.1 onwards. Policies could get incorrectly reordered impacting traffic, because load update do configuration file loaded.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related to all UI tools (mgd-bsd/cli-bsd, XML and DMI</b>
<a href="#">1630167</a> Minor	Zeroize RPC returns no positive reply Product-Group=junos Severity=Minor	Zeroize RPC returns no positive reply
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: QFX RCB issues</b>
<a href="#">1589942</a> Minor	The management interface speed is reflected as 10G instead of 1G Product-Group=junos Severity=Minor	On VMHost platforms, the management interface speed is displayed as 10G instead of 1G. There is no fi fixes PR1589942 and PR1636668. Make sure both are included.
<b>PR</b>	<b>Synopsis</b>	<b>Category: MX10K linecard</b>

<b>Number</b>		
<a href="#">1785182</a> Minor	On Junos MX and SRX platforms silent FPC reboot is observed with no generation of crash files Product-Group=junos Severity=Minor	On Junos platforms with MPC7E, MPC8E, MPC9E, LC1201, LC480, MS-SPC3, SRX5K-SPC3 cards. When one memory issue, the line card reboots silently without generating any crash files.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: MX10K platform</b>
<a href="#">1772508</a> Minor	ISSU or Standard Installation will be aborted with error "mgd: error: Check-out failed for IPF daemon (/usr/sbin/ipfd) without details" Product-Group=junos Severity=Minor	On all MX platforms except MX240, MX480, MX960 and VMX platforms, "mgd: error: Check-out failed for details" errors will be observed while performing Unified in-service software upgrade (ISSU) and ISSU or and software installation will fail.
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: video monitoring feature</b>
<a href="#">1822738</a> Major	The PFE becomes inactive or disabled when running multicast in a video monitoring setup Product-Group=junos Severity=Major	On all Junos MX platforms with MPC2E, MPC3E, MPC4, MPC5 and MPC6 line cards and video monitoring c Forwarding Engine(PFE) goes in to disabled state when multicast traffic with more than 10 downstream
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Virtual Private LAN Services</b>
<a href="#">1729052</a> Major	The rpd process crash will be observed during VPLS to EVPN migration Product-Group=junos Severity=Major	On all Junos platforms during VPLS (Virtual Private LAN Service) to EVPN (Ethernet Virtual Private Netw are configured under the same routing instance and "instance-type evpn" is enabled, then upon deactiv the IFL configuration associated with VPLS will lead to rpd process crash.
<a href="#">1774580</a> Major	Multicast traffic loop will be observed when Multicast traffic is sent over the Access Interface marked as CCC-DOWN Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms in the VPLS (Virtual Private LAN Service) Multi-homing with Multi looping will be observed due to L2 (Layer 2) Multicast traffic being sent on the access interface status r
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Virtual Router Redundancy Protocol</b>
<a href="#">1760534</a> Minor	VRRP Status displayed incorrectly in CLI command Product-Group=junos Severity=Minor	On Junos and Junos OS Evolved platforms with dual RE, when GRES and NSR are enabled. VRRP status i VRRP is configured although it is in the correct state. There is no impact with services. its a display issu
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Windsurf fabric software</b>
<a href="#">1830457</a> Critical	On Junos MX2020 platform with non-native LC, HSL2 'failed word alignment' error causes the fabric planes to go in check state Product-Group=junos Severity=Critical	On Junos MX2020 platform with non-native LCs (Line Cards) such as MPC-4/5/7 or MS-MPC, post FPCs (F fabric planes goes into check state due to HSL2 (High Speed Link Version 2) 'failed word alignment' erro goes down hence there will be partial traffic impact through the impacted PFE and fabric-plane combir
<a href="#">1835860</a> Major	Fabric plane goes into check state and alarm is consistently seen along with traffic drop when ADC based line cards are restarted on certain MX platforms Product-Group=junos Severity=Major	On MX2010/MX2020 platforms having adapter cards MPC7E and MPC5E with SFB3 (Switch Fabric Boards) seen when both the ADC cards are restarted, which then causes a fabric link error on the adjacent ADC for FPC (Flexible Physical Interface Cards Concentrators)/PFE (Packet Forwarding Engine) plane combin
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: usf flow and datapath issue on SPC3</b>

<a href="#">1844731</a> Major	High heap memory caused MX-SPC3 PIC to go offline Product-Group=junos Severity=Major	On Junos platforms, specifically MX240, MX480 and MX960 supporting MX-SPC3 service cards, if inline-jf routes (~4M routes) resulting in kernel memory exhaustion that is high Heap Memory and SPC3 Pic goes
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: usf nat related issues</b>
<a href="#">1776355</a> Major	Internet traffic destined for the NAT pool address (Network Address Translation) will loop after configuration changes Product-Group=junos Severity=Major	On Junos MX platforms, with MS-MPC and SPC3 service cards, Change in "interim-logging-interval" config looped and it will impacting CPU utilisation and traffic drop can be seen.
<a href="#">1802242</a> Major	Interim logs for deterministic NAT are not generated as per the modified time interval Product-Group=junos Severity=Major	On all MX platforms, the configuration change done to interim logging interval for deterministic Network come into effect. Even after modifying the interval value from T1 to T2, logs still get generated at the

## 21.2R3-S9 - List of Known issues

<b>PR Number</b>	<b>Synopsis</b>	<b>Category: 5G CUPS - PFCP subscriber</b>
<a href="#">1634966</a> Major	When all configured anchor PFEs are offline on the SAEGW-u, there may be a peer association mis-match between the SAEGW-u and SAEGW-c Product-Group=junos	If all configured anchor PFEs are offline, SAEGW daemon stops replying to PFCP heartbeat requests. The control peer will interpret this as as loss of connectivity to the user plane device and may not send PFCP Association Release Request. This may result in the control-peer association to remain on the SAEGW-u, but removed from the SAEGW-c  <i>Resolved In:</i> junos:21.3R2 junos:21.3R3 junos:21.4R2 junos:22.1R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: "agentd" software daemon</b>
<a href="#">1802050</a> Minor	Telemetry streaming fails due a race condition under certain scenarios such as RE mastership switchover or restart chassis-control Product-Group=junos	On all platforms configured with gRPC and GNMI based telemetry, it is observed that due to race condition between two processes called JSD and mgd-api, streaming is failing under several scenarios like RE (Routing Engine) mastership switchover, restart chassis-control etc.  <i>Resolved In:</i> evo:22.3R3-S3-EVO evo:24.2R1-EVO evo:24.3R1-EVO junos:20.3X75-D440 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.4R2 junos:24.2R1 junos:24.3R1
<a href="#">1855112</a> Major	Telemetry streaming during ISSU (upgrading pre 22.1 image to 22.1+) Product-Group=junos	In 22.1, JUNOS telemetry infrastructure under gone an enhancement in its message infrastructure. Due to this enhancement, telemetry streaming is not advisable during ISSU (upgrading pre 22.1 image to 22.1+).  <i>Resolved In:</i>
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: access node control protocol daemon</b>
<a href="#">1814300</a> Major	L2BSA sessions remain down when port messages from ANCP neighbor are dropped in a scaled scenario after ISSU followed by GRES Product-Group=junos	On all Junos MX platforms with dual RE (Routing Engine), having ANCP (Access Node Control Protocol ) and L2BSA (Layer 2 Bitstream Access) sessions under a scaled scenario (about 10k subscribers), when ISSU (Unified In-Service Software Upgrade) is performed followed by a GRES (Graceful Routing Engine Switchover), it is observed that the port-up messages from ANCP neighbor are dropped either at PFE (Packet Forwarding Engine) or by the ANCP daemon or BBE (Broadband Edge)/autoconf plugin which causes L2BSA sessions to remain down and as a result traffic over the affected subscriber sessions are dropped.  <i>Resolved In:</i> evo:24.2R2-EVO evo:24.4R1-EVO evo:25.1R1-EVO junos:23.2R2-S3 junos:23.4R2-S3 junos:24.2R2 junos:24.3R1 junos:24.4R1 junos:25.1R1

PR Number	Synopsis	Category: This gnats category is required to track NG-SPC PRS for SBU
<a href="#">1841859</a> Major	High traffic on MX-SPC3 will cause PIC to go down Product-Group=junos	On Junos platforms, specifically MX240, MX480 and MX960 supporting MX-SPC3 (Services Processing Card) service cards, if PIC (Physical Interface Cards) receives high traffic enough to make CPU (Central processing unit) almost 100% busy, it will go down, triggers flowd core-dump and cause network impact.  <i>Resolved In:</i> junos:21.4R3-S10 junos:22.2R3-S6 junos:22.4R3-S6 junos:23.2R2-S3 junos:23.4R2-S4 junos:24.2R2 junos:24.4R1 junos:25.1R1
PR Number	Synopsis	Category: This category is for Broadband Edge accounting related issue
<a href="#">1643077</a> Major	High CPU usage might be seen post ISSU Product-Group=junos	On all Junos platforms, In a Layer 2 vpn scenario, High CPU usage can be seen after ISSU is performed.  <i>Resolved In:</i> evo:21.3R3-EVO evo:21.4R2-EVO evo:22.1R1-EVO evo:22.2R1-EVO junos:21.2R3 junos:21.3R3 junos:21.4R2 junos:22.1R1 junos:22.2R1
PR Number	Synopsis	Category: BBE database related issues
<a href="#">1818781</a> Major	Multiple BBE daemons getting killed automatically on MX platforms Product-Group=junos	In a scaled subscriber management router, customers observe authd and Jdhcpd daemons being killed automatically due to block tasks.  <i>Resolved In:</i> junos:23.2R2-S2 junos:23.2R2-S3 junos:24.2R2 junos:24.3R1 junos:24.4R1
PR Number	Synopsis	Category: BBE interface related issues
<a href="#">1631646</a> Minor	The knob "host-prefix-only" may not take effect after enabling it under underlying interface of subscribers Product-Group=junos	On MX platform with enhanced subscriber management enabled, when "host-prefix-only" is configured on the underlying-interface for subscribers, it might not work in FPC.  <i>Resolved In:</i> evo:22.1R1-EVO
<a href="#">1650974</a> Minor	The bbe-smgd crash can be seen in a certain scenario Product-Group=junos	On Junos MX platforms supporting subscriber services, the bbe (broadband edge)-smgd (subscriber management daemon) crash can be observed when more than 1725 (eg 1726 and greater) PS (Pseudowire) interfaces are configured. There can be an impact on subscriber services due to the crash but the system self-recovers.  <i>Resolved In:</i> evo:21.4R3-EVO evo:22.1R2-EVO evo:22.2R2-EVO evo:22.3R1-EVO junos:21.4R3 junos:22.1R2 junos:22.2R2 junos:22.3R1
<a href="#">1849552</a> Minor	FPC crash upon change of tunnel-services bandwidth Product-Group=junos	On MX platforms with MPC5/MPC7 line cards when there are active pseudo wire subscribers and there is a change in the tunnel-services bandwidth configuration, FPC (Flexible Physical Interface Card Concentrators) crash is observed with the subsequent impact on the traffic.  <i>Resolved In:</i>
PR Number	Synopsis	Category: MIBs related to BBE
<a href="#">1709029</a> Minor	CLI command 'show snmp mib walk ascii' is not showing the correct output for jnxSubscriberPicCountTable and jnxSubscriberSlotCountTable Product-Group=junos	In a subscriber-management environment SNMP polling of jnxSubscriberPicCountTable and jnxSubscriberSlotCountTable MIBs will result in a single line of output if any subscribers terminated over ps interface are present.  <i>Resolved In:</i> evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
<a href="#">1824274</a> Minor	The jnxSubscriberPortTerminatedCounter shows incorrect values for interfaces Product-Group=junos	On Junos MX platforms, the jnxSubscriberPortTerminatedCounter no longer shows the correct values for the individual ports. It shows the same value for all ports. These subscribers are enabled over PS interface.  <i>Resolved In:</i> evo:24.2R2-EVO evo:24.4R1-EVO junos:23.2R2-S4 junos:23.4R2-S2-J5 junos:23.4R2-S3-J17 junos:23.4R2-S3-J4 junos:23.4R2-S4-J11 junos:23.4R2-S5 junos:24.2R2 junos:24.4R1
PR Number	Synopsis	Category: BBE Statistics daemon & libraries

<a href="#">1814017</a> Minor	Extensible Subscriber Services Manager (ESSM) sessions gets disconnected when PFE encounters an issue for any service or subscriber session Product-Group=junos	On all Junos and Junos OS Evolved platforms, where subscriber-management is configured and if PFE encounters an issue for any service or subscriber session then it sends an error for anyone of the session in bulk response which results in the subscriber services to be disconnected.  <i>Resolved In:</i> evo:24.2R2-EVO evo:24.3R1-EVO evo:24.4R1-EVO junos:23.2R2-S4 junos:24.2R2 junos:24.3R1 junos:24.4R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Bi Directional Forwarding Detection (BFD)</b>
<a href="#">1598786</a> Critical	After first parallel ISSU aborts, subsequent ISSU attempts on failed node aborts with 'Aborting Daemon Prepare' Product-Group=junos	On all platforms supporting ISSU (In-Service Software Upgrade), if ISSU is performed on two routers connected over LFM (Link Fault Management), the process is aborted with 'Aborting Daemon Prepare' on one of the routers. The BFD (Bidirectional Forwarding Detection) process gets stuck at Abort state and is not reverted back to Idle state. Any subsequent attempt of ISSU on failed node fails with the same message.  <i>Resolved In:</i> junos:21.4R1 junos:22.1R1
<a href="#">1706018</a> Minor	The BFD session would flap when the GRES is triggered with single-hop BFD over AE interfaces configured Product-Group=junos	On all Junos and Junos Evolved platforms, Bidirectional Forwarding Detection (BFD) sessions would flap and leads to route churn in the network when the Graceful Routing Engine Switchover (GRES) is triggered with single-hop BFD sessions over Aggregated Ethernet (AE) interfaces. It is a timing issue.  <i>Resolved In:</i> evo:22.3R3-EVO evo:22.4R2-EVO evo:23.1R2-EVO evo:23.2R1-EVO junos:21.2R3-S8-J15 junos:21.4R3-S3 junos:22.2R3-S3 junos:22.3R3 junos:22.4R2 junos:23.1R2 junos:23.2R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Border Gateway Protocol</b>
<a href="#">1663883</a> Major	Traffic loss will be seen due to delay in BGP convergence time Product-Group=junos	On all Junos and Junos Evolved platforms, whenever there is high percentage of background CPU usage that causes the rpd process to run at an average CPU load, BGP convergence will be slow, which results in traffic loss.  <i>Resolved In:</i> evo:21.4X1-EVO evo:22.3R2-EVO evo:22.3R3-EVO evo:22.3X80-D33-EVO evo:22.4R1-EVO evo:23.4R1-EVO junos:18.2X75-D67 junos:20.3X75-D50 junos:22.3R2 junos:22.3R3 junos:22.4R1 junos:23.4R2 junos:24.1R1
<a href="#">1670630</a> Major	The rpd crashes upon receiving BGP multi-nexthops inetflow route in the 21.4 software release and onward Product-Group=junos	On all Junos and Junos Evolved platforms, when a BGP (Border Gateway Protocol) inetflow route is received with multiple next-hops in the 21.4 software release and onwards, the rpd will crash and a core dump file will be generated.  <i>Resolved In:</i> evo:21.4R3-EVO evo:22.1R3-EVO evo:22.2R2-EVO evo:22.3R1-EVO evo:22.4R1-EVO junos:21.4R3 junos:22.1R3 junos:22.2R2 junos:22.3R1 junos:22.4R1
<a href="#">1690213</a> Major	BMP will not send EOR message for BMP RIBOUT monitoring in certain case. Product-Group=junos	On all Junos and Junos Evolved platforms, BGP Monitoring Protocol (BMP) will not send End of RIB (EOR) message for BMP RIBOUT monitoring in certain case for some releases. This is a timing related problem specific to BMP RIBOUT monitoring and not applicable for other monitoring type (RIB-IN or Local RIB monitoring). This will impact some data collections.  <i>Resolved In:</i> evo:22.2R3-EVO evo:22.3R2-EVO evo:22.4R2-EVO evo:23.1R1-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:22.1R3-S4 junos:22.2R3 junos:22.3R2 junos:22.4R2 junos:23.1R1 junos:23.2R1 junos:23.3R1
<a href="#">1719498</a> Major	In MPLS L3VPN-BGP multipath scenario route calculation or recalculation causes the rpd process to crash Product-Group=junos	On all Junos and Junos Evolved platforms, memory leak is observed in Multi-protocol Label Switching (MPLS) Layer3 and labelled routes scenario when Border Gateway Protocol (BGP) with multipath is configured. Multiple route changes and deletion overtime that triggers this memory leak can lead the rpd to run out of memory causing the rpd process to crash.  <i>Resolved In:</i> evo:21.4R3-S4-EVO evo:22.1R3-S3-EVO evo:22.2R3-S1-EVO evo:22.3R3-EVO evo:22.3X50-EVO evo:22.3X80-D38-EVO evo:22.3X80-D39-EVO evo:22.4R2-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:21.4R3-S2-J16 junos:21.4R3-S2-J22 junos:21.4R3-S4 junos:21.4R3-S5 junos:21.4R3-S6 junos:22.1R3-S3 junos:22.2R3-J7 junos:22.2R3-S1 junos:22.3R3 junos:22.4R2 junos:22.4R3 junos:22.4R3-S1 junos:23.1R2 junos:23.2R1 junos:23.3R1 junos:24.2R2
<a href="#">1807504</a> Major	BGP multipath selects wrong interface with "Multiple Single-Hop EBGP sessions on different links using the same IPv6 Link-Local Address"	On Junos and Junos Evolved Platforms having BGP (Border Gateway Protocol) Multipath when "Multiple Single-Hop EBGP Sessions on different links using the same IPv6 (Internet Protocol Version 6) Link-Local Address" as over multiple links and one of those links is down, the next-hop information which has the smallest IFL (Logical Interface) index interface will get deleted. Since RIB (Routing Information Base) and FIB (Forwarding Information Base) are not correct network traffic will be lost

	Product-Group=junos	when one of the peer device is down.  <i>Resolved In:</i> evo:22.4R3-S5-EVO evo:23.2R2-S3-EVO evo:23.4R2-EVO evo:24.2R1-EVO evo:24.2R2-EVO evo:24.3R1-EVO evo:24.4R1-EVO junos:22.4R3-S5 junos:23.2R2-S3 junos:23.4R2 junos:24.2R1 junos:24.2R2 junos:24.3R1 junos:24.4R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: EVO L2 Control Plane PRs</b>
<a href="#">1644651</a> Major	MAC address might not be learnt on the directly connected Interface Product-Group=junos	On all Junos OS Evolved platforms on a directly connected AE interface, the MAC address might not be learned. There are rare chance during multiple commits for VLAN membership change  <i>Resolved In:</i> evo:20.4R3-S3-EVO evo:20.4X10-EVO evo:21.3R3-EVO evo:21.4R2-EVO evo:22.1R2-EVO evo:22.2R1-EVO junos:20.4R3-S3 junos:21.3R3 junos:21.4R2 junos:22.1R2 junos:22.2R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: EVPN control plane issues</b>
<a href="#">1675054</a> Critical	Junos OS and Junos OS Evolved: RPD core upon receipt of a specific EVPN route by a BGP route reflector in an EVPN environment (CVE-2022-22219) Product-Group=junos	Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering a routing protocol daemon (RPD) crash, leading to a Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. Please refer to <a href="https://kb.juniper.net/JSa69898">https://kb.juniper.net/JSa69898</a> for more information.  <i>Resolved In:</i> evo:21.4R3-EVO evo:22.1R1-S2-EVO evo:22.1R3-EVO evo:22.2R2-EVO evo:22.3R1-EVO evo:22.4R1-EVO junos:21.3R3-S2 junos:21.4R2-S2 junos:21.4R3 junos:22.1R1-S2 junos:22.1R3 junos:22.2R2 junos:22.3R1 junos:22.4R1
<a href="#">1789065</a> Major	Deleting/adding EVPN Instance and interface having ESI configuration resulting in traffic loss Product-Group=junos	On Junos and Junos Evolved platforms in the EVPN-VPWS (Ethernet Virtual Private Network - Virtual Private Wire Service) Multihoming single active scenario, high CPU utilization is observed for a long time (5 mins) when EVPN triggers full BGP (Border Gateway Protocol) RIB (Routing Information Base) evaluation in a scaled setup (5 million prefixes) where BGP imports entire internet routing tables for deleting/adding EVPN Instance and Interface having ESI (Ethernet Segment Identifier) configuration. Traffic flow convergence from Active PE (Provider Edge) to Backup PE happens because backup PE elects itself as DF (Designated Forwarder) and interface CCC (Circuit Cross-Connect) is not marked down. If traffic is received from a VPLS (Virtual Private LAN Service) peer then the Backup PE device is unable to forward traffic to VPWS Remote PE as it doesn't have an EVPN-VPWS tunnel established with remote PE i.e. results in traffic loss.  <i>Resolved In:</i> evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R2-EVO evo:24.2R1-EVO junos:23.2R1-S1-J6 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R2 junos:24.2R1
<a href="#">1839959</a> Critical	The MAC+IP table and mac-table are not in sync in the EVPN-MPLS active-active multihomed scenario leading to traffic loss Product-Group=junos	On all Junos and Junos OS Evolved platforms that supports ESI lag interface and in an EVPN-MPLS (Ethernet Virtual Private Network - Multi Protocol Label Switching) active-active multihomed scenario, when the multihomed access interfaces are flapped in quick succession, it results in an unresolved destination route for the specific IP host. This is occurred due to race condition within l2ald (Layer 2 Address learning daemon) followed by an interface flap which causes the locally learned MAC to go missing from the mac-table on the other PE router.  <i>Resolved In:</i> evo:21.4R3-S10-EVO evo:22.2R3-S6-EVO evo:22.4R3-S7-EVO evo:23.2R2-S4-EVO junos:21.4R3-S10 junos:21.4R3-S4-J26 junos:22.2R3-S6 junos:22.4R3-S7 junos:23.2R2-S4 junos:23.4R2-S4 junos:23.4R2-S5 junos:24.4R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: EVPN Layer-2 Forwarding</b>
<a href="#">1766275</a> Major	EVPN CRB traffic drops after the FPC restart Product-Group=junos	On all Junos platforms, in Ethernet Virtual Private Network - Multiprotocol Label Switching (EVPN-MPLS) setup, with high scale and churn caused in the system by local Flexible PIC Concentrators (FPCs) restart, indirect next hop creation will fail for EVPN Centrally-Routed Bridging (CRB) instances and EVPN CRB traffic will be forwarded as Broadcast, Unknown Unicast, and Multicast (BUM) traffic. If there is any filter configured to drop BUM traffic explicitly, then traffic drop will be seen. Otherwise, the impact will be a traffic flood which will not cause traffic loss.  <i>Resolved In:</i> evo:23.4R2-EVO evo:24.1R1-EVO junos:23.4R2 junos:24.1R1 junos:24.2R2
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: EX interfaces issues</b>

<a href="#">1580560</a> Major	On EX2300, EX3400, :EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent. Product-Group=junos	On EX2300, EX3400, :EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent.  <i>Resolved In:</i>
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: EX4400 platform</b>
<a href="#">1734435</a> Major	Error handling for SMBus access routines Product-Group=junos	On Junos Platforms, there may be functionality such as: PoE configuration not working, BFD flap, delayed or no response from sensors, Optics etc, but the device would be responsive.  <i>Resolved In:</i> junos:21.4R3-S4 junos:21.4R3-S6 junos:22.1R3-S3 junos:22.2R3-S1 junos:22.3R2-S2 junos:22.3R3-S1 junos:22.4R2-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.2R2 junos:23.3R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Express PFE including evpn, vxlan</b>
<a href="#">1808040</a> Minor	VRRP multicast packets coming from external hosts connected to the EVPN-VXLAN fabric might get duplicated on QFX10k platforms Product-Group=junos	On QFX10k platforms having Seamless EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) DCI (Data Center Interconnect) Stitching configured with L2 (Layer 2) Bridged Overlay design, VRRP (Virtual Router Redundancy Protocol) multicast traffic may be flooded to all RNVEs (Regular Network Virtualization Equipment) and Wan-VTEPs (Wide Area Network - Virtual Tunnel Endpoints), irrespective of DF (Designated Forwarder)/NDF (Non-Designated Forwarder) role. This may result in duplicates of VRRP multicast packets.  <i>Resolved In:</i> junos:21.4R3-S9 junos:22.2R3-S4 junos:22.3R3-S4 junos:22.4R3-S3 junos:23.2R2-S2 junos:23.4R2 junos:24.2R1 junos:24.2R2 junos:24.3R1 junos:24.4R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Express PFE L2 fwding Features</b>
<a href="#">1798887</a> Major	Traffic drops are observed in the EVPN-VXLAN environment having IPv4 and IPv6 address configured in underlay Product-Group=junos	On Junos QFX10002-36Q/QFX10002-72Q/QFX10002-60C and PTX10002-60C platforms, the decapsulate of the VXLAN (Virtual eXtensible Local-Area Network) packet will fail and result in traffic drops due to the tunnel termination table not being programmed in PFE (Packet Forwarding Engine).  <i>Resolved In:</i> junos:21.4R3-S8 junos:22.2R3-S4 junos:22.3R3-S4 junos:22.4R3-S3 junos:23.2R2-S2 junos:23.4R2 junos:24.2R1 junos:24.2R2 junos:24.3R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Express PFE L3 Multicast</b>
<a href="#">1636842</a> Minor	Multicast traffic received on the INET interface might be dropped Product-Group=junos	On QFX10002-60c, in EVPN/VxLAN scenario multicast traffic received on the INET interface (L3 interface) might be dropped.  <i>Resolved In:</i> junos:20.4R3-S4 junos:21.4R3 junos:22.2R2 junos:22.3R1 junos:22.4R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Express PFE MPLS Features</b>
<a href="#">1683123</a> Minor	L3VPN to VXLAN traffic gets dropped on QFX platforms with QFX10000-60S-6Q and QFX10000-36Q line cards Product-Group=junos	On QFX10008 and QFX10016 platforms with QFX10000-60S-6Q and QFX10000-36Q line cards installed, L3VPN (Layer 3 VPN) to VXLAN (Virtual Extensible LAN) traffic will not flow if the L3VPN tunnel is terminated on the affected cards.  <i>Resolved In:</i> junos:20.4R3-S5
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: SRX4100/SRX4200 platform software</b>
<a href="#">1808353</a> Major	Traffic drop is seen when "monitor traffic interface" command is issued for an interface on Junos SRX platforms Product-Group=junosvae	On Junos SRX4100/SRX4200 platform, starting and stopping the "monitor traffic interface", causes the VPN tunnel or tagged traffic to be dropped. However, keeping the "monitor traffic interface" running, ensures that traffic will function properly. Issue occurs when monitor interface command on an interface is performed on devices that has vlan-tagging configured.  <i>Resolved In:</i> junos:21.4R3-S9 junos:22.2R3-S5 junos:22.4R3-S4 junos:23.2R2-S2 junos:23.4R2-S3 junos:24.2R1-S1 junos:24.2R2 junos:24.3R1 junos:24.4R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: MX10K LC2101 Timing</b>

<a href="#">1719966</a> Minor	"clksync_zl3068x_get_tod_time: Failed with error :1" error message seen after indus linecard reboot Product-Group=junos	These logs doesn't impact any functionality. It is an expected case and has been taken care of with this fix.  <i>Resolved In:</i> evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:22.4R2 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: BSDX Software installation issues</b>
<a href="#">1713187</a> Major	JSU: request system software delete reboot does not trigger a reboot Product-Group=junos	On all Junos platforms, request system software delete reboot does not trigger a reboot. The JSU functionality is working and JSU package is getting deleted as expected. Manual reboot is required.  <i>Resolved In:</i> junos:23.2R2 junos:23.3R1 junos:23.4R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: ISIS routing protocol</b>
<a href="#">1667575</a> Major	When the SPF algorithm for IS-IS in Segment Routing use case is triggered frequently, CPU usage might increase Product-Group=junos	On all Junos and Junos Evolved platforms, when the shortest-path-first (SPF) algorithm for IS-IS is triggered frequently, CPU usage might increase and impact the device performance and traffic.  <i>Resolved In:</i> evo:22.4R1-EVO junos:22.4R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: jpppd daemon</b>
<a href="#">1488302</a> Minor	MPLS VPN label can point to the discard next hop after a Routing Engine switchover without NSR if the egress interface is pp0 Product-Group=junos	The traffic (which is destined to the hosts behind static PPPoE subscriber's CPE device) drop is seen due to bad MPLS VPN label (which points to discard next-hop) after RE switchover without NSR. The traffic destined to the CPE device itself is not affected.  <i>Resolved In:</i> junos:17.4R2-S11
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: IPSEC/IKE VPN</b>
<a href="#">1762463</a> Minor	The system boots into amnesiac mode or rescue mode if HSM is disabled/enabled during vSRX reboot Product-Group=junos	On Junos OS vSRX platforms with HSM (Hardware Security Module) integrated, in a race condition, if HSM is disabled/enabled and taking more time (more than 60 Secs) to return failure (retry mechanism before declaring HSM connectivity failure) during vSRX reboot window, the system boots into amnesiac mode or rescue mode (if rescue configuration has been configured by administrator).  <i>Resolved In:</i> evo:22.3R3-S3-EVO evo:22.3X50-EVO evo:22.4R0-J0-EVO evo:22.4R3-EVO evo:23.2R2-EVO evo:23.4R1-S1-EVO evo:23.4R2-EVO junos:21.4R3-S10 junos:22.2R3-S5 junos:22.3R3-S2 junos:22.3R3-S3 junos:22.4R3 junos:22.4R3-S1 junos:23.2R2 junos:23.4R1-S1 junos:23.4R2 junos:24.2R1
<a href="#">1817228</a> Major	IPsec VPN traffic disruption after a change of Authentication protocol is seen on platforms running kmd process Product-Group=junos	On all Junos platforms that run kmd process, IPsec VPN tunnels experience traffic disruption after a change of authentication protocol (ESP is change to AH or vice versa).  <i>Resolved In:</i> junos:21.2R3-S7-J19 junos:21.4R3-S9 junos:22.2R3-S5 junos:22.4R3-S6 junos:23.2R2-S3 junos:23.4R2-S3 junos:24.2R2 junos:24.3R1 junos:24.4R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Security platform jweb support</b>
<a href="#">1725808</a> Critical	Junos OS: J-Web: Multiple vulnerabilities resolved in PHP software (CVE-2023-0567, CVE-2023-0662, CVE-2023-3823, CVE-2023-3824, CVE-2023-0568) Product-Group=junos	PHP software included with Juniper Networks Junos OS J-Web has been updated to resolve multiple vulnerabilities. Please refer to <a href="https://supportportal.juniper.net/JSA88120">https://supportportal.juniper.net/JSA88120</a> for more information.  <i>Resolved In:</i> evo:23.3R2-EVO junos:21.4A3 junos:21.4R3-S8 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R1-S2 junos:23.2R2 junos:23.2R2-S2 junos:23.3R2 junos:23.4R1 junos:23.4R1-S2 junos:23.4R2 junos:24.1R1 junos:24.2R1 junos:24.3R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: PFE infra to support jvision</b>
<a href="#">1706155</a> Minor	The PFE fabric telemetry data(128.0.0.xx->128.0.0.1 udp 2000) was forwarded to data port Product-Group=junos	The packets with internal ip address 128.0.0.xx -> 128.0.0.1 and upd port 2000 might be forwarded out the default egress interfaces. Such packets are telemetry data for PFE fabric sensor, which should be sent to routing-engine only.

Resolved In: junos:23.2R2 junos:23.4R2 junos:24.1R1

PR Number	Synopsis	Category: Label Distribution Protocol
<a href="#">1670334</a> Minor	Traffic loss will be seen in an LDP->BGP-LU stitching scenario Product-Group=junos	On all QFX platforms, traffic loss can happen when the BGP-LU (Labeled Unicast) routes are exported to LDP (Label Distribution Protocol) to perform LDP->BGP-LU stitching, on a device with directly connected BGP peers.  <i>Resolved In:</i> evo:22.1R3-EVO evo:22.2R3-EVO evo:22.3R2-EVO evo:22.4R1-EVO evo:23.1R1-EVO junos:20.4R3-S5 junos:21.4R3-S2 junos:22.1R3 junos:22.2R3 junos:22.3R2 junos:22.4R1 junos:23.1R1
PR Number	Synopsis	Category: lldp sw on MX platform
<a href="#">1811545</a> Major	The LLDP neighborhood does not recover on AE interfaces Product-Group=junos	When LLDP is configured on interface all and there are AE interfaces configured, to disable LLDP on one of the AE "set protocols lldp interface is done". To enable it back when rollback is done for reverting disable config, AE is not participating in LLDP neighborhood and this happening because PFE stopped sending packets to control plane because on rollback L2CPD did not sent LLDP ENABLE for its child interface to PFE and LLDP on child interface was still set to disabled for PFE.  <i>Resolved In:</i> evo:22.2R3-S7-EVO evo:22.3X50-EVO evo:22.4R3-S6-EVO evo:23.2R2-S3-EVO evo:23.4R2-EVO evo:24.2R1-S2-EVO evo:24.2R2-EVO evo:24.3R1-EVO evo:24.4R1-EVO junos:21.2R3-S7-J17 junos:21.2R3-S8-J2 junos:22.2R3-S7 junos:22.4R3-S6 junos:23.2R2-S3 junos:23.4R2-S4 junos:24.2R1-S2 junos:24.2R2 junos:24.3R1 junos:24.4R1
PR Number	Synopsis	Category: MPC11 ULC interface software related issues.
<a href="#">1852016</a> Major	picd core hit on mpc11 while Verifying GRES and FH stages after injecting errors Product-Group=junos	@jjli Wherever this PR is not fixed please make a release note of it  <i>Resolved In:</i> junos:22.2R3-S6
PR Number	Synopsis	Category: Multicast for L3VPNs
<a href="#">1700345</a> Major	The rpd crash happens when Multicast VPN (Virtual Private Network) is configured with separate route-targets scenario Product-Group=junos	This happens only when MVPN protocol has separate route targets configured and then both the address families are disabled. rpd (Routing process daemon) infra parsing does not check if MVPN protocol is disabled and hence will create the auto policies for route-targets if configured. So if those policies are not marked as active in MVPN configuration flow, it does not get resolved and thereby the policy object may not be valid thus leading to the core.  <i>Resolved In:</i> evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO junos:22.4R3 junos:23.1R2 junos:23.2R1
PR Number	Synopsis	Category: MX10K platform
<a href="#">1674322</a> Minor	SNMP traps "Power Supply failed" and "Power Supply OK" are not generated Product-Group=junosvae	On all Junos MX10k and PTX10k platforms, when a PSU with no feeds connected, but the DIP switch at the back of the PSU is set in a position where it expects the feeds to be connected, then POWER FAILED TRAPS might not get generated as expected.  <i>Resolved In:</i> evo:22.1R3-EVO evo:22.2R2-EVO evo:22.3R2-EVO evo:22.4R1-EVO junos:20.3X75-D36 junos:20.4R3-S5 junos:21.2R3-S6 junos:22.1R3 junos:22.2R2 junos:22.3R2 junos:22.4R1 junos:23.1R1
PR Number	Synopsis	Category: OS IPv4/ARP/ICMPv4
<a href="#">1801129</a> Major	IP routes can get added to a deleted routing table Product-Group=junos	On all Junos platforms routes can get added to deleted routing tables.  <i>Resolved In:</i> junos:24.2R2 junos:24.3R1
PR Number	Synopsis	Category: JUNOS Network App Infrastructure (for ping, traceroute, etc)
<a href="#">1746779</a> Minor	show system connections show-routing-instances; reports all	Show system connections show-routing-instances; reports all routing-instances as unknown.

routing-instances as unknown.  
Product-Group=junos

*Resolved In:* junos:20.3X75-D52 junos:21.4R3-S6 junos:22.1R3-S4 junos:22.2R3-S3 junos:22.3R3-S2 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R2 junos:23.4R1

PR Number	Synopsis	Category: Express Paradise PFE Sflow
<a href="#">1672121</a> Minor	Flow sample packet is not sent to the collector when the destination is an ECMP path Product-Group=junos	On QFX10k platforms with sflow configured, flow sample packet is not sent to the collector when a packet is received on an Integrated Routing and bridging (IRB) interface and its destination is an Equal Cost Multi Path (ECMP) path.  <i>Resolved In:</i> junos:20.4R3-S5 junos:22.1R3 junos:22.2R2 junos:22.3R2 junos:22.4R1
PR Number	Synopsis	Category: Periodic Packet Management Daemon
<a href="#">1702687</a> Major	The ppmmd process crash will be seen after GRES Product-Group=junos	On all Junos and Junos OS Evolved platforms with dual Routing Engines, after back-to-back GRES is performed, the ppmmd process crashes.  <i>Resolved In:</i> evo:22.3X50-EVO evo:22.3X80-D43-EVO evo:22.3X80-D44-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.2R2-EVO junos:23.1R2 junos:23.2R1
PR Number	Synopsis	Category: QFX5K Timing software
<a href="#">1848071</a> Major	The PTP BC is not working and stays in 'FREERUN' state. Product-Group=junos	The PTP BC is not working and stays in 'FREERUN' state. PTP slave is not locking to upstream master.  <i>Resolved In:</i> junos:21.4R3-S10 junos:24.2R2 junos:24.4R2 junos:25.1R1
PR Number	Synopsis	Category: rosen-6 and rosen-7 mvpn bugs
<a href="#">1736328</a> Major	RPD core@bgp_rt_terminate_job->bgp_process_rt_terminate->bgp_rt_terminate_subr->bgp_rto_adv_q_free->bgpg_rt_open () Product-Group=junos	This is a day one code and is seen only in the scale setup with specific configuration with both l2vpn and rosen mvpn configuration present, when the scale configurations are done and then deleted (load baseline config). As per existing implementation, the MDT table though not required for l2vpn instances was being created and this code has been there since day one and in normal cases this should not create any issues. However in this scaled configs setup, when all configs were deleted, bgp global and group specific tables were getting to inconsistent state specifically for the MDT table and hence the issue.  <i>Resolved In:</i> evo:23.2R2-S3-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:23.2R2-S3 junos:23.4R2 junos:24.1R1
PR Number	Synopsis	Category: Issues related to dynamic-tunnels routing infrastructure
<a href="#">1728305</a> Critical	The tunnel remains down and traffic is impacted due to no validation of the tunnel forwarding route Product-Group=junos	Traffic drop is observed when the tunnel route resolves over a route, which the next hop was set to discard. This occurs as there is no check if the nexthop is of type discard, reject or black hole.  <i>Resolved In:</i> evo:22.2R3-S1-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:20.3X75-D43 junos:21.4R3-S5 junos:22.2R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.2R2 junos:23.3R1
PR Number	Synopsis	Category: RPD Interfaces related issues
<a href="#">1722809</a> Minor	Router Send RA with Router lifetime 0 when the upstream interface is shut Product-Group=junos	For virtual interfaces used in EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) with multihoming scenario and VRRP (Virtual Router Redundancy Protocol), after receiving RA (Router Advertisement) packet with lifetime zero, host VM deletes the default route to the VGA (Virtual Gateway address) address and hence traffic loss is observed.  <i>Resolved In:</i> evo:22.2R3-S1-EVO evo:22.2R3-S3-EVO evo:22.3R3-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:22.2R3-S1 junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
<a href="#">1741485</a> Major	Unnecessary rsync messages causing issues Product-Group=junos	<i>Resolved In:</i> evo:24.1R1-EVO junos:24.1R1
PR	Synopsis	Category: Issue related to mcnh routing infrastructure within RPD

<b>Number</b>		
<a href="#">1708299</a> Minor	The rpd process crash is seen with scaled multicast next-hops Product-Group=junos	On all Junos OS Evolved platforms, due to timing issues in scaled setup with multicast next-hops, the rpd process might crash when the corresponding multicast next-hops Aggregated Ethernet (AE) interface flaps continuously. This will result in traffic loss.  <i>Resolved In:</i> evo:21.4R3-S3-EVO evo:22.2R2-S2-EVO evo:23.2R1-EVO junos:23.2R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: RPD Next-hop issues including indirect, CNH, and MCNH</b>
<a href="#">1746964</a> Major	EVPN type-5 doesn't work properly when route resolution is performed with preserve-nexthop-hierarchy enabled Product-Group=junos	On all Junos and Junos Evolved platforms, with preserve-nexthop-hierarchy enabled, when EVPN type-5 route resolution is performed, it is observed that protocol-nexthop address is missing in the cache database, and next-hop paths are not created. This will cause traffic to be sent to the wrong host since the next-hop is not created.  <i>Resolved In:</i> evo:22.4R3-EVO evo:23.2R2-EVO evo:23.3R2-EVO evo:23.4R1-EVO evo:24.1R1-EVO junos:22.4R3 junos:22.4R3-S1 junos:23.2R2 junos:23.2R2-J14 junos:23.3R2 junos:23.4R1 junos:24.1R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: RPD route tables, resolver, routing instances, static routes</b>
<a href="#">1740175</a> Major	Memory leak is seen once on the standby RE when restart routing is performed on the master RE Product-Group=junos	On all Junos and Junos Evolved platforms configured with NSR (Nonstop Active Routing) and BGP (Border Gateway protocol) rib-sharding, it is observed that whenever the rpd process is restarted on the master RE (Routing Engine), memory leak occurs once on the standby RE. There is no impact due to this issue.  <i>Resolved In:</i> evo:23.2R2-EVO evo:23.4R1-EVO evo:24.1R1-EVO junos:22.3R3-S2 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.4R1 junos:24.1R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: show route table commands, tracing, and syslog facilities</b>
<a href="#">1644319</a> Major	The openconfig network-instance/protocols/static-routes/static id list-key might generate an error on encoding through NETCONF Product-Group=junos	On all platforms, the field corresponding to the identifier of the static route if expressed in IPv6 format through NETCONF encoding/translation could generate some issues. Hence the configuration will not get translated to Junos CLI.  <i>Resolved In:</i> evo:21.4R2-EVO evo:21.4R3-EVO evo:22.1R2-EVO evo:22.2R1-EVO evo:22.3R1-EVO junos:21.4R2 junos:21.4R3 junos:22.1R2 junos:22.2R1 junos:22.3R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Generic platform and infra issues for MS-MIC and MS-MPC(XLP)</b>
<a href="#">1700462</a> Major	mshpmand crashes after loading a new image Product-Group=junos	On MX platform, Once the device is loaded with the new image, PIC tries to boot up. mshpmand is one of the processes inside PIC, crashes sometimes.  <i>Resolved In:</i>
<a href="#">1827806</a> Major	mshpmand crash on clear/show services sessions parallel in high scale on MX platforms Product-Group=junos	On Junos MX with MS-MPC/MS-MIC cards, when clear service sessions are executed from multiple windows (approx 5 terminals), the PIC reboots and eventually all the service traffic will be impacted.  <i>Resolved In:</i> junos:21.2R3-S6-J16 junos:21.4R3-S9 junos:22.2R3-S5 junos:22.4R3-S4
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: SRX branch platforms</b>
<a href="#">1811858</a> Minor	Monitored-Status keeps Up after CTL link down in branch model SRX HA Product-Group=junos	After CTL link down, Monitored-Status in "show chassis cluster interfaces" keeps showing "Up" state.  <i>Resolved In:</i> junos:21.4R3-S10 junos:22.2R3-S6 junos:22.4R3-S5 junos:23.2R2-S2 junos:23.4R2-S3 junos:24.2R1-S2 junos:24.2R2 junos:24.3R1 junos:24.4R1
<a href="#">1821368</a> Major	DAC interface does not send fault signal to a peer device when the DAC interface is admin disabled Product-Group=junos	On SRX380 platform, when a DAC interface is admin disabled, the DAC interface does not send a fault signal to a peer device and on peer device it will reflect as up.  <i>Resolved In:</i> junos:23.4R2-S3 junos:24.2R1-S2 junos:24.2R2 junos:24.3R2 junos:24.4R1
<a href="#">1841080</a> Major	Xe interfaces link down when IP address is assigned Product-Group=junos	On SRX380 platforms configured for packet-mode operation and an IP address is assigned to xe (10 Gigabit ethernet) interfaces, the interface link status will go to down state.

*Resolved In:* junos:21.4R3-S10 junos:22.2R3-S5 junos:22.4R3-S6 junos:23.2R2-S3 junos:23.4R2-S3 junos:24.2R1-S2 junos:24.2R2 junos:24.4R1 junos:25.1R1

<a href="#">1848557</a> Major	Local or peer device's interface reflects down after SRX380's reboot Product-Group=junos	On SRX380 platforms, the local interface status or the peer device's interface reflects down after SRX380's reboot when both devices are configured with auto-negotiation on the SRX380's 4x10GbE ports.  <i>Resolved In:</i> junos:22.2R3-S7 junos:22.4R3-S6 junos:23.2R2-S3 junos:23.2R2-S4 junos:23.4R2-S4 junos:24.2R2 junos:24.2R2-S1 junos:24.4R1 junos:24.4R2 junos:25.1R1 junos:25.2R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: MPC7E, MPC8E and MPC9E timing and synchronization</b>
<a href="#">1803105</a> Major	PTP attribute changes on upstream device causes best clock master slot switchover Product-Group=junos	On all MX platforms(except MX80) with multi line card chassis, when PTP slave or stateful streams are configured across multiple linecards with clock from same PTP time provider and the announce msg parameters changes from the upstream device, the best master clock (BMC) slot switchover is observed and is restored back within few seconds. Although the slot time interval is very less, it can still lead to major impact as the active PTP slot and clock path is switched over and results in re-routing of the clocks.  <i>Resolved In:</i> evo:24.4R1-EVO evo:25.1R1-EVO junos:24.4R1 junos:24.4R2 junos:25.1R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: ZT/YTpfe bridging, learning, stp, oam, irb software</b>
<a href="#">1854428</a> Major	JDI-RCT:M/Mx: Redbull-Dviata: Error messaes observed @ aftd-trio[16588]:[Error] Em: root: Insert entry failed, entry:parentToken:2566839 entryMask:fffffffffffffff index:52 Data:0x7f8eb5c59500 Product-Group=junos	When "clear bridge mac table" is triggered on a scaled system, the inject of callout to trigger flushing of mac entries fails for some BDs on some PFEs resulting in the error reported. Fix of this is available through PR <a href="https://gnats.juniper.net/web/default/1664694#external_tab">https://gnats.juniper.net/web/default/1664694#external_tab</a> and is available from 22.3R3  <i>Resolved In:</i>
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Trio pfe I3 forwarding issues</b>
<a href="#">1864237</a> Critical	Observing out-of-order packets when the TCP traffic gets passed over AE bundle and tunnelled via MPLSoUDP tunnel Product-Group=junos	On Junos OS platforms, When "dynamic tunnels" configured and "set chassis loopback-dynamic-tunnel" knob is used and when TCP (Transmission Control Protocol) traffic passed via MPLSoUDP (Multi-Protocol Label Switching Over User Datagram Protocol) tunnel through an outgoing AE (Aggregated Ethernet) bundle interface having member interfaces, use of either inner or outer header hash calculations lead to out-of-order packets at the egress. It causes service impact on related flow of traffic due to out-of-order packets.  <i>Resolved In:</i> evo:24.4R2-EVO evo:25.2R1-EVO junos:21.2R3-S5-J52 junos:23.4R2-S3-J16 junos:23.4R2-S5 junos:24.2R2-S1 junos:24.4R2 junos:25.1R1 junos:25.2R1
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Configuration mgmt, ffp, load-action, commit processing</b>
<a href="#">1751574</a> Major	Netconf RPC commit fails due to commit warning received for unprotect operation, CLI commit completes with warning Product-Group=junos	In Netconf private edit configuration session, commit RPC fails when unprotect operation is performed.  <i>Resolved In:</i>
<b>PR Number</b>	<b>Synopsis</b>	<b>Category: Issues related to NETCONF</b>
<a href="#">1585855</a> Critical	< ok/> response is getting generated along with < rpc-error> Product-Group=junos	When maximum-password-length is configured and the user tries to configure password whose length exceeds configured maximum-password-length, there is an error and the " tag is emitted. (Ideally " tag should not be emitted in an error scenario.) The configuration does not get committed.  <i>Resolved In:</i> evo:22.2R3-S1-EVO evo:22.3R2-S2-EVO evo:22.3X50-EVO evo:22.3X80-D43-EVO evo:22.3X80-D44-EVO evo:22.4R3-EVO evo:23.1R1-EVO evo:23.2R1-EVO junos:20.3X75-D36 junos:22.1R3-S6 junos:22.2R3-S1 junos:22.3R2-S2 junos:22.3R3-S1 junos:22.4R2-S2 junos:22.4R3 junos:23.1R1 junos:23.2R1 junos:23.4R2
<b>PR</b>	<b>Synopsis</b>	<b>Category: Virtual Router Redundancy Protocol</b>

Number		
<a href="#">1674069</a> Major	JDI-RCT:MPC10E@errors@fpc1 user.err aftd-trio: [Error] INLINEKA : Invalid anchor nexthop: 594 for VRRP key IfIndex : 487 group : ip : seen after restart fpc with PDT test configs. Product-Group=junos	Error logs related to invalid anchor next hops are seen when the MPC10/11 FPCs are restarted with distributed ae irb VRRP sessions. The AE should span multiple fpcs.  <i>Resolved In:</i>
PR Number	Synopsis	Category: usf flow and datapath issue on SPC3
<a href="#">1799512</a> Major	Traffic impact on SPC3-PIC due to high throughput and bursty traffic Product-Group=junos	On Junos MX platforms equipped with SPC3 (Services Processing Card 3), when running on Talus 0x215 version and each SPC3-PIC (Physical Interface Card) handling significantly high throughput along with bursty traffic, will lead to tx_NoDp_drop' to be hit leading to packet drop.  <i>Resolved In:</i> evo:24.2R2-EVO evo:24.3R1-EVO evo:24.4R1-EVO junos:21.4R3-S8 junos:22.2R3-S5 junos:22.3R3-S4 junos:22.4R3-S3 junos:23.2R2-S1 junos:23.4R2 junos:24.2R1 junos:24.2R2 junos:24.3R1 junos:24.4R1