21.3R3-S5: Software Release Notification for JUNOS Software Version 21.3R3-S5

Alert Description

Junos Software Service Release version 21.3R3-S5 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

Solution

Junos Software service Release version 21.3R3-S5 is now available.

21.3R3-S5 - List of Fixed issues

PR Number	Synopsis	Category: JUNOS bugs found in UAC integration
1692398	Connection fails are observed on Junos despite a valid auth entry Product-Group=junos	On Junos platforms, authentication failures and connection drops are observed for a few users when UAC (Unified Access Control) modules fail to look up the roles.
PR Number	**Synopsis**	**Category: EX4300 PFE**
1720219	PFE process crash is observed on Junos EX4300 platforms Product-Group=junos	In a rare scenario, due to timing issues, the Packet Forwarding Engine (PFE) crash is observed on Junos EX4300 platforms. This causes traffic loss until the PFE comes up.
1722284	Native VLAN traffic is getting dropped in the Q-in-Q scenario on EX4300 Product-Group=junos	On Junos EX4300-24T/24P when the native CVLAN (Customer Virtual Local Area Network) ID is configured for Q-in-Q setup, the traffic for that particular VLAN gets dropped even if the knob "input-native-vlan-push" is configured. This issue is encountered when the when inner-tag matches 'native-vlan-id' irrespective of the outer tag.
1725042	VRRP peers delay to sync when 'mac-move-limit' is configured on EX switch Product-Group=junos	On Junos EX series platforms, VRRP (Virtual Router Redundancy Protocol) sync will be delayed impacting the VRRP traffic if the device receives a VRRP packet when setting up the 'mac-move-limit' configuration.
1729636	Traffic loss is seen after configuration changes related to VSTP are committed Product-Group=junos	On EX4300 platforms, when RSTP (Rapid Spanning Tree Protocol) and VSTP(VLAN Spanning Tree Protocol) are configured on two different interfaces which are part of the same VLAN (Virtual LAN), the RSTP-enabled interface will drop traffic after doing a configuration change in VSTP for the specified VLAN.
PR Number	**Synopsis**	**Category: EX4300 Platform**

1738406	On EX4300MP-EX4300 mixed VC setup, "show system software sets" command shows 'Pending set' software version even after rebooting. Product-Group=junos	On EX4300MP-EX4300 mixed VC setup, "show system software sets" command shows 'Pending set' software version even after rebooting.
1749289	On EX4300, "Error requesting CMTFPC SET INTEGER" and "Error requesting SET BOOLEAN" logs may be seen after device boot up. There is no functional impact for the error messages Product-Group=junos	
PR Number	**Synopsis**	**Category: EX4300 HA (GRES, NSR, NSB)**
1665562	EX4300-48MP: VC: NSSU aborted with Backup RE maybe in inconsistent state Product-Group=junosvae	For NSSU to work fix should be present in the Base image. The issue started from 21.4R2 onwards. e.g If NSSU is done from 21.4 to 22.2 fix should be present in 21.4 image.
PR Number	**Synopsis**	**Category: EX4300 Platform implementation**
1712785	EX4300-48MP CPLD firmware fails to upgrade from 2.2 to 2.5 with 22.4R1.10 image Product-Group=junosvae	EX4300-48MP CPLD firmware fails to upgrade from 2.2 to 2.5 with 22.4R1.10 image
PR Number	**Synopsis**	**Category: EX2300/3400 PFE**
1742303	DHCP packets traversing the switch even though the source mac is not present in accept-source-mac list Product-Group=junos	In EX2300 & EX3400 devices, even though accept-source-mac knob is configured, DHCP Packets with the MAC address not present in the accept-source-mac list are accepted and traverse in the network.
PR Number	**Synopsis**	**Category: EX2300/3400 platform**
1737524	VC on EX3400 platforms will not form with 40GBASE-BXSR optics Product-Group=junos	On Junos EX3400 platforms, the Virtual Chassis will not form if 40GBASE-BXSR optics are used on VCPs (Virtual Chassis ports).
PR Number	**Synopsis**	**Category: EX-Series VC Infrastructure**
1700133	One of the Virtual Chassis members on EX4600-VC might be disconnected during VC initialization Product-Group=junos	On EX4600-VC, when "request system reboot all members" is executed, post-reboot one of the VC member/Flexible PIC Concentrator(FPC) might disconnect and join the VC back due to Packet Forwarding Engine (PFE) restart. Traffic loss is seen when FPC is disconnected.
PR Number	**Synopsis**	**Category: SRX DNS DGA and tunneling related**
1732028	The DNS cache gets wiped out due to the flowd crash on all SRX platforms after the upgrade Product-Group=junos	The flowd crashes after upgrading all SRX platforms to 21.2R3 and later releases when DNSF plugin (SecIntel/ATP Cloud) is running along with Security-Metadata-Streaming DNS policy configuration. It causes the DNS (Domain Name System) cache to get wiped out.

PR Number	Synopsis	Category: Accounting Profile
1692411	Error messages are observed and incorrect values are returned for SNMP requests for pfe traffic statistics Product-Group=junos	pfed: PFED_NOTIF_GLOBAL_STAT_UNKNOWN: xxxx in syslog The above log messages will be seen when we are using SNMP and if its trying to poll "show pfe statistics notification" through MIB OID - 1.3.6.1.4.1.2636.3.44.1.1.2.1.2.
PR Number	**Synopsis**	**Category: ACX L3 IPv4, IPv6 support**
1707932	L2VPN traffic is dropped as the default MTU is less by 4 bytes Product-Group=junos	On Junos ACX platforms, due to Maximum Transmission Unit (MTU) mismatch, L2VPN (Layer 2 Virtual Private Network) traffic will be dropped on the egress interface facing Customer Edge (CE).
PR Number	**Synopsis**	**Category: ACX MPLS**
1720827	The Forwarding Engine Board (FEB 0) crashes and impacts traffic when the L2circuit IGP primary path port is down Product-Group=junos	On Junos ACX1000, ACX1100, ACX2000, ACX2100, ACX2200, and ACX4000 platforms, the Forwarding Engine Board (FEB 0) will crash when the L2circuit Interior Gateway Protocol (IGP) primary path port on the local device is down. Sub-minute traffic loss is seen when FEB 0 crashes. This issue is seen only when 'hot-standby' mode is in place for L2circuit and not seen with just 'standby' mode.
PR Number	**Synopsis**	**Category: AFT l2lam**
1721704	Sending GARP reply packet on a VTEP interface causes flooding in network on QFX5130 and QFX5700 platforms Product-Group=junos	On Junos OS Evolved QFX5130 and QFX5700 platforms, Gratuitous Address Resolution Protocol (GARP) flooding occurs in the network when it receives a GARP reply packet on a Virtual Tunnel End Point (VTEP) interface.
PR Number	**Synopsis**	**Category: MPC Fusion SW**
1744883	100G interfaces will flap due to RE switchover on Junos MX platforms with MPC3E-3D-NG/MPC-3E-3D-NG-Q linecards Product-Group=junos	On Junos MX platforms with MPC3E-3D-NG/MPC-3E-3D-NG-Q linecards, 100G interfaces will flap due to RE (Routing Engine) switchover.
PR Number	**Synopsis**	**Category: Application Quality of Experience**
1743107	flowd process crash observed in Junos branch SRX platforms Product-Group=junos	This issue is observed on Junos SRX platforms supporting SD-WAN (Software-defined Wide Area Network) like SRX300, SRX320, SRX340, SRX345, SRX380, SRX550, SRX1500, SRX4100, SRX4200, SRX4600, SRX5600, SRX5800, cSRX and vSRX in AppQoE (Application Quality of Experience) scenario where the passive probe session of SD-WAN is not closed gracefully. This results in flowd crash and impacts user traffic.
PR Number	**Synopsis**	**Category: A15 specific issue**
1738188	Failover can be seen on SRX5K cluster with SPC2	On all SRX5000 series platforms with SPC2 cards configured in a

	cards while executing RSI Product-Group=junos	chassis cluster, when RSI is being collected which has the command 'i2csc fpc' in the script, an interrupt storm generates a CB (Control Board) alarm which triggers a failover. Intermittent traffic disruption could be seen till the failover is complete.
PR Number	**Synopsis**	**Category: dynamic vlan creation and associated processing**
1743903	If more than 32 vlan ranges are configured under the dynamic-profile then login issue and traffic impact can be seen with subscribers of random VLANs Product-Group=junos	On all Junos platforms that support subscriber services, when more than 32 VLAN ranges are configured, random VLAN (Virtual Local Area Network) traffic is impacted and subscribers are unable to login.
PR Number	**Synopsis**	**Category: BBE packet trigger access model issues**
1726136	PTSP subscribers are stuck in 'configured' state Product-Group=junos	On MX platforms supporting packet-triggered subscribers and policy control (PTSP) feature, a high percentage of packet triggered subscribers are getting stuck in 'Configured' state due to an authentication failure.
PR Number	**Synopsis**	**Category: the SMGD redundancy plugin in SMGD**
1718342	In a DHCP ALQ subscriber scenario delete-binding-on-renegotiation knob does not work as expected due to a synchronization error between the primary and the backup routers Product-Group=junos	On Junos platforms, active lease query (ALQ) synchronization between peers is not happening properly. Traffic forwarding impact would be observed if there was a switchover from the Primary to the Backup. The primary router will correctly delete-binding-on-renegotiation and create a new session, but the backup router keeps the old session and old MAC address. (DHCP overrides have delete-binding-on-renegotiation configured and work as expected on the primary router whereas no notification is sent to the backup to delete the session)
PR Number	**Synopsis**	**Category: Border Gateway Protocol**
1626717	Junos OS and Junos OS Evolved: An rpd crash may occur when BGP is processing newly learned routes (CVE-2023-44197) Product-Group=junos	An Out-of-Bounds Write vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA73163 for more information.
1670715	The rpd process crash is observed when running BGP-LS EPE configuration with RIB sharding enabled Product-Group=junos	The rpd process crash is observed when running BGP-LS (Border Gateway Protocol - Link-State) EPE (Egress Peer Traffic Engineering) configuration with RIB sharding enabled since the label allocation is only allowed in the main thread. But the shards thread was trying to allocate the label during EPE configuration parsing.
1679495	RV task replication will be stuck in the "NotStarted" state when routing-options validation is deactivated/activated Product-Group=junos	On all Junos and Junos Evolved platforms with Non-Stop Routing (NSR) enabled, in a rare case, Route Validation (RV) task replication will be stuck in the "NotStarted" state when routing-options validation is deactivated/activated.
1687887	More than expected traffic loss is seen with ECMP FRR enabled during link down scenario Product-Group=junos	On all Junos and Junos Evolved platforms, in a link down/BFD (Bidirectional Forwarding Detection) down event traffic loss is seen to occur more than the expected with ECMP (Equal-Cost

		Multipath) FRR (Fast Reroute) or BGP PIC (Prefix-Independent Convergence) configured.
1709837	Junos OS and Junos OS Evolved: A crafted BGP UPDATE message allows a remote attacker to de-peer (reset) BGP sessions (CVE-2023-4481) Product-Group=junos	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA72510 for more information.
1712527	The PE advertises incorrect next-hop towards CE although BGP export policy configured with next-hop under policy-statement Product-Group=junos	The show route advertising-protocol bgp reporting nexthop self rather than IP in the configured policy-statement for next-hop.
1728455	The rpd process crashes when BGP is cleaned up Product-Group=junos	On Junos and Junos OS Evolved platforms, if static default RT-C (Route Target -Constrain) is configured when Border Gateway Protocol (BGP) is cleaned up (whole BGP is cleaned up), the routing process will crash.
1728604	Traffic impact is seen when there is a single peer in the proxy BGP group connected to the BGP route reflector Product-Group=junos	On all Junos and Junos OS Evolved platforms, if the proxy BGP (Border Gateway Protocol) route reflector is connected to the only peer present in the BGP group then it stops advertising the routes coming from the remote cluster and that leads to proxy route-target routes not getting added which causes traffic disruption.
1732493	The rpd process crash will be observed with BMP and independent resolution is enabled for secondary BGP routes Product-Group=junos	On all Junos and Junos OS Evolved platforms, when BMP (BGP Monitoring Protocol) post-policy and independent resolution is enabled for secondary (route leaked through rib-group) BGP routes, then with the inactive secondary route change the rpd process crash will be observed.
1732833	Constant BGP peer flaps would core rpd Product-Group=junos	On all Junos and Junos OS Evolved platforms , rpd (Routing Protocol Daemon) soft cores can be seen if BGP (Border Gateway protocol) peer session flaps constantly. It is non Service impacting issue.
1736029	Junos OS and Junos OS Evolved: RPD crash when attempting to send a very long AS PATH to a non-4-byte-AS capable BGP neighbor (CVE-2023-44186) Product-Group=junos	An Improper Handling of Exceptional Conditions vulnerability in AS PATH processing of Juniper Networks Junos OS and Junos OS Evolved allows an attacker to send a BGP update message with an AS PATH containing a large number of 4-byte ASes, leading to a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA73150 for more information.
1739335	The rpd process crash will be observed when the prefix-limit exceeds on the backup RE Product-Group=junos	On all Junos and Junos OS Evolved platforms configured with BGP (Border Gateway Protocol), NSR (Nonstop Active Routing), and prefix-limit with idle-timeout, when the prefix-limit exceeds on the backup RE (Routing Engine) and switchover is performed the rpd process crash will be observed on the new backup RE.
1739919	Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute (CVE-2023-0026) Product-Group=junos	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA71542 for more details.

1745073	CPU in rpd spikes and scheduler slips will be observed when the duplicate community is added Product-Group=junos	On all Junos and Junos Evolved platforms, when Border Gateway Protocol (BGP) is configured with the existing community member added via another community that is called in import policy and the intermediate router does not support large/extended communities based on scale (route). Due to this, the rpd Central Processing Unit (CPU) stays high and protocols level choking will be seen in adjacent nodes. Scheduler slips are also observed due to the same.
PR Number	**Synopsis**	**Category: BBE Remote Access Server**
1709574	The subscriber sessions will be logged out when assigned IP addresses from Radius or AAA via framed-IP Product-Group=junos	On the MX platforms, when the subscriber sessions are not assigned addresses from locally configured pools and the knob "address-protection" is not enabled under the access profile configuration, then those subscriber sessions will be logged out after GRES with termination code: "aaa shutdown-administrative-reset".
PR Number	**Synopsis**	**Category: Class of Service**
1722939	Cos Scheduling hierarchy on PS interface is destroyed when the TCP is modified Product-Group=junos	When a TCP attached on a service IFL is modified, cosd is supposed to destroy the hierarchy and send gencfg messages (gencfg message used for storing configuration values) with new TCP information. LT IFD :: level1 PS transport IFL :: level2 --> TCP attached here is modified. PS service IFL :: level3 After destroying the hierarchy of level2 and level3 mentioned above, instead of sending the add message which will rebuild the hierarchy, it sends a change message, thus the new hierarchy is not built up while old hierarchy is destroyed. As the PS interface hierachy is destroyed because of the events mentioned above, eventhough TCP is present for the service/transport IFL, LT IFD queues would be used for sending the PS traffic.
1734013	The CoS scheduler map will not get attached to the sub-interface correctly when shaping-rate and scheduler-map are configured on it Product-Group=junos	On all MX platforms, when shaping-rate and scheduler-map are configured on a sub-interface and a wildcard expression for sub-interfaces is used in the class-of-service interface definition, then the CoS (Class of Service) scheduler map will not get attached as per the configuration to the sub-interface and will not work correctly. Example: set class-of-service interfaces unit * classifiers.
PR Number	**Synopsis**	**Category: Enhanced Broadband Edge support for cos**
1713968	Subscribers connectivity is lost due to multiple MIC restart on all Junos MX platforms with MPC5E and BBE configuration Product-Group=junos	On all Junos MX platforms with MPC5E and BBE (Broadband Edge) configuration, subscribers connectivity will be lost due to multiple MIC (Modular Interface Card) restart.
PR Number	**Synopsis**	**Category: Captive Portal**
1736937	Junos OS: EX Series: A PHP vulnerability in J-Web allows an unauthenticated attacker to control important environment variables (CVE-2023-36844) Product-Group=junos	A PHP External Variable Modification vulnerability in J-Web of Juniper Networks Junos OS on EX Series allows an unauthenticated, network-based attacker to control certain, important environments variables. Utilizing a crafted request an attacker is able to modify certain PHP environments variables leading to partial loss of integrity, which may allow chaining to

		other vulnerabilities. For more information see https://kb.juniper.net/JSA72300
PR Number	**Synopsis**	**Category: L2NG Access Security feature**
1724933	On certain Junos EX and QFX platforms the static ARP entries for DHCP-security are not present Product-Group=junos	On certain Junos EX series switches, the static MAC (Media Access Control) bindings are not present in certain conditions. This issue will be seen when the static DHCP (Dynamic Host Configuration Protocol)-security ARP(Address Resolution Protocol) bindings are moved from an interface having a higher interface number to an interface with a lower interface number. Due to the binding not happening, there will be impact on the traffic. The workaround when such a binding change is done is to restart the DHCP services after the configuration is committed.
PR Number	**Synopsis**	**Category: Device Configuration Daemon**
1679952	After changing the settings related interface, a particular interface does not flap but a LAG interface may flap on all Junos platforms except MX Product-Group=junos	The LAG (Link Aggregation Group) member links may flap on all Junos platforms except MX when the configuration of any interface is changed/modified. The flap is not seen always.
1692404	Incompatible/unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss Product-Group=junos	On all Junos platforms, while performing the Junos upgrade from the release before 20.4 to a higher version having an incorrect configuration may fail. This issue may lead to traffic loss or network outages.
1714267	The interface speed gets set to a lower speed when the interface is disabled and enabled because renegotiation of the interfaces happens at the previously negotiated speed Product-Group=junos	On Junos platforms with MPC line cards, negotiated interfaces will try to come up with the speed already negotiated instead of using the original interfaces speed even if re-negotiation happens like reinserting cable.
1726073	PFE table is not updated when new VLANs are added in an AE bundle when ESI is enabled Product-Group=junos	IFF Change message is not propagated to PFE when AE (Aggregated Ethernet) bundle has ESI (VPLS/EVPN) configuration.
PR Number	**Synopsis**	**Category: Firewall Filter**
1749092	High CPU utilization of the mib2d process will be observed with error messages due to stale SNMP requests Product-Group=junos	On all Junos platforms, high CPU utilization, up to 100%, of the mib2d process will be observed with error messages and this may also result in a crash/core when memory gets exhausted due to a gradual increase in stale SNMP (Simple Network Management Protocol) requests.
PR Number	**Synopsis**	**Category: ACX IFL, IFF creation**
1691004	The PFE process crashes on ACX5448 Product-Group=junos	On Junos ACX5448 platforms, the PFE (Packet Forwarding Engine) process will crash after continuous IFD (Interface Device) flaps. As a result, all traffic will be lost until the process recovers on its own.
PR Number	**Synopsis**	**Category: DNX VPLS**

1722919	Intermittent MAC move is observed in VPLS environment when ACX5448 or ACX710 is acting as a PE device Product-Group=junos	On Junos ACX5448 and ACX710 platforms acting as a PE (Provider Edge) device in a VPLS (Virtual Private LAN Services) environment and multiple CE (Customer Edge) interfaces are bound to a single routing instance, intermittent MAC move is observed. This is a corner case scenario and the MAC move can be triggered due to various reasons and not limiting to mac address time out, L2 loop on the extended network or a congested backbone link connecting the PE devices. The split horizon rule in VPLS fails and the traffic received from VPLS LSI (Label-Switched Interface) is forwarded back towards the MPLS core through the LSI.
PR Number	**Synopsis**	**Category: Issues related to NTP issues on evo**
1729126	Junos OS and Junos OS Evolved: Multiple NTP vulnerabilities resolved Product-Group=junos	Multiple NTP vulnerabilities have been resolved in Juniper Networks Junos OS and Junos OS Evolved by updating third-party software where vulnerabilities were found during external security research. Please note that there is no ability within the CLI to perform any exploitation for these issues. Only shell allows sending ntpq queries to remote systems. Please refer to https://supportportal.juniper.net/JSA73177 for more information.
PR Number	**Synopsis**	**Category: EVPN control plane issues**
1716663	RPD process crash may be observed when routing or evo-pfemand process is restarted and multicast snooping process adds a route to inetmcsn.1 table Product-Group=junos	On Junos OS Evolved platforms, a routing process crash may be observed when "restart routing" or "restart evo-pfemand" is applied and multicast snooping process adds a route to inetmcsn.1 table at the same time. When the issue is hit, the core file of rpd will be generated. This is a timing issue and it may be observed when both the events happen at the same time.
1723832	The rpd core is seen in the long-running devices with EVPN enabled Product-Group=junos	On Junos and Junos Evolved platforms, BGP (Border Gateway Protocol) community object reference count is not handled properly during the process of remote BGP peer routes update event. The community reference count is increasing during the increment function. However, decrement functions are not called in one of the places after processing the routes update. This will lead to a disturbance of the continuity reference count, which will cause an rpd crash.
PR Number	**Synopsis**	**Category: EVPN Layer-2 Forwarding**
1758677	Traffic flooding for MAC addresses programming failure Product-Group=junos	Issue 1: On QFX5K and EX platforms, traffic flooding will be observed for MAC addresses not getting programmed in hardware in the VXLAN (Virtual Extensible LAN) environment with VPLAG (Virtual Chassis Port Link Aggregation) configured and BGP (Border Gateway Protocol) flaps. This issue happens when hardware write by L2ALM to PFE fails, and during re-sync, SVLBNH (shared VXLAN load balancing next hop) info is not sent to PFE/hardware. Issue 2: On all Junos platforms, l2alm sends a delete request for control MAC addresses to l2ald after multiple hardware sync failures.

PR Number	Synopsis	Category: EX4100 PFE
1699216	Traffic impact is observed when OSPF adjacency gets stuck in exstart or exchange state Product-Group=junos	On Junos EX4100 platform the OSPF (Open Shortest Path First) adjacency establishment will take longer time with more than 90 VRRPv6 (Virtual Router Redundancy Protocol for IPv6) sessions causing traffic disruption.
1738404	[QFX5/EX] Error message like 'BRCM-VIRTUAL,brcm_vxlan_port_discard_set(),13034:Failed to set bcm_port_discard_set to 0 for port (61) err(Invalid unit) Product-Group=junos	You might see the error message like 'BRCM-VIRTUAL,brcm_vxlan_port_discard_set(),13034:Failed to set bcm_port_discard_set to 0 for port (61) err(Invalid unit)' in a Virtual Chassis. The Error is no functional impact.
PR Number	**Synopsis**	**Category: EX4400 PFE software**
1716902	IGMP/MLD queries may get dropped if received on a port on the backup VC member when IGMP/MLD snooping is enabled Product-Group=junos	On Junos QFX and EX in the VC (Virtual Chassis) scenario, when the switch is acting as pure L2 (Layer 2), and forwarding IGMP (Internet Group Management Protocol)/MLD (Multicast Listener Discovery) query as transit traffic, if IGMP/MLD snooping is enabled then IGMP/MLD queries may get dropped if received on a port on the backup VC member resulting in IGMP/MLD groups to expire.
1718286	DHCP services are impacted as DHCP binding will not work as expected Product-Group=junos	On all Junos and Junos Evolved platforms, all the DHCP (Dynamic Host Configuration Protocol) security services will be impacted as the DHCP-security binding will not work if the DHCP server-facing interface is a VTEP (VXLAN tunnel endpoint) interface.
1731522	The traffic drop will be observed after changing the VSTP VLAN configuration Product-Group=junos	On Junos EX4400, EX4100, EX2300, EX3400, and QFX5K platforms, traffic drop would happen on RSTP (Rapid Spanning Tree Protocol) enabled port attached to a VLAN (Virtual Local Area Network) when the same VLAN has VSTP (VLAN Spanning Tree Protocol) enabled on a different port and there is a configuration change done on VSTP for that VLAN.
1731548	The fxpc process crashes when the next hop information is not properly maintained in the PFE table Product-Group=junos	On Junos EX series deployed as a virtual chassis, post switchover/GRES (Graceful Routing Engine Switchover), next hop information for Type 5 route fluctuates which leads to invalid entries in the PFE (Packet Forward Engine) table and causes the fxpc (Packet Forwarding Engine Manager) process to crash.
1732271	Filter term dropping VRRP traffic when "then log" is configured Product-Group=junos	On all Junos platforms, VRRP (Virtual Router Redundancy Protocol) packet goes to a wrong CPU queue when filter is added to match VRRP packet with "then log" action, resulting in VRRP functionality impact.
1733365	Error logs are seen with a non-vxlan dot1x enabled port Product-Group=junos	In a heaviliy loaded system in a specific scenario (Dot1x in multiple supplicant mode & dynamic vlan from radius server & non vxlan access port) following log message may be captured in the syslog - {brcm_as_dot1x_vxlan_set_mac_learning_mode:1168 dot1x bd_get failed for bd index 0}. This log is not impacting any funtionality.
1736790	EX4400 shaping rate not working as expected	On EX platforms shaping rate on 100gig link over 70g not

	Product-Group=junos	working as expected.
1747095	LLDP will not work on HGoE VC mode with 40G VCP connections Product-Group=junos	On EX4400/QFX5120 platforms, having High Gigabit over Ethernet (HGoE) Virtual Chassis (VC) mode in the master, when VC members are connected by 40G links, Link Layer Discovery Protocol (LLDP) Bridge Protocol Data Unit (BPDU) from VC master destined to the remote VC members (more than one-hop away) are dropped at VCP interface due to Virtual LANs (VLANs) membership check.
1749312	Connectivity fails intermittently on 802.1x enabled ports Product-Group=junos	On EX4100 and EX4400 platforms performing as Virtual Chassis, host authentication will get stuck in connecting state if 802.1x dynamic VLAN single supplicant mode is enabled on access switch port and complete traffic towards that port will be dropped.
1757329	The dcpfe process crash will be seen when L2PT interfaces are configured with multiple protocols Product-Group=junos	On QFX5K/EX4100/EX4400 platforms that support Layer 2 protocol tunneling (L2PT), sending the bi-directional traffic on those interfaces and deleting/re-adding the L2PT multiple times causes the dcpfe crash which triggers Packet Forwarding Engine (PFE) restart.
PR Number	**Synopsis**	**Category: EX4400 platform**
1696444	Transceiver not detected after it's unplugged and plugged in again Product-Group=junos	On EX4400 and EX4300MP platforms, after JOJI (jack out/jack in), transceiver is not detected in "show chassis hardware".
1707762	BFD/LACP flaps will be seen on EX4400 platforms Product-Group=junos	On EX4400 platforms, BFD (Bidirectional Forwarding Detection) will flap randomly along with LACP (Link Aggregation Control Protocol) flaps or VC (Virtual Chassis) connection loss.
1720257	EX4400 shows incorrect interface et-0/0/0 Product-Group=junos	On EX4400-48MP/EX4400-24MP pic 0 port 0 ifd (Interface device) would be incorrect due to set chassis fpc <> pic <> port <> speed <> configuration.
1753576	Runt frames generate excessive traffic statistics on EX4100/EX4400 platforms Product-Group=junos	On EX4100/EX4400 platforms with Multi-rate gigabit ethernet (MGE) ports , incorrect register is read for the runt counter and the calculation logic generates a big value. As these bytes are part of input octets, it displays incorrect value.
PR Number	**Synopsis**	**Category: Express PFE CoS Features**
1645488	Junos ACX/PTX/QFX platforms might silently discard packets after an interface flaps Product-Group=junos	On certain ACX Series, PTX Series, or QFX Series devices running Junos OS, the device might silently discard packets when the backoff time is set on port or with congestion during link down and up events. There will be a service impact because of the traffic drops. As restoration, the egress Flexible PIC Concentrator (FPC) needs to be rebooted.
1719956	Convergence delay is seen when FPC is offlined under heavy traffic and scaled scenario Product-Group=junos	On Junos PTX3000, PTX5000, PTX10008, and PTX10016 routers, when the Flexible PIC Concentrator (FPC) is offlined with scale configuration and heavy traffic, a delay in convergence (into tens of minutes) is seen on all the live FPCs in the chassis other than the offlined one. This impacts traffic.

1738981	DSCP classifier is not created on IP interfaces Product-Group=junos	On Junos QFX10k platforms, on configuring diffServ code point (DSCP) classifier and when inet or inet6 is configured with custom dot1p on interface, default dscp classifiers are not getting removed properly.
PR Number	**Synopsis**	**Category: Express PFE FW Features**
1716398	Junos OS: PTX Series and QFX10000 Series: Received flow-routes which aren't installed as the hardware doesn't support them, lead to an FPC heap memory leak (CVE-2023-22392) Product-Group=junos	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA73530 for more information.
1727067	FPC crashes when the firewall filter is configured with above 65k prefixes in a single filter Product-Group=junos	On the below PTX platforms (PTX1000, PTX3000 (NextGen), PTX5000, PTX10008, PTX10016 and QFX10002), when prefixes above 65K are configured in a single firewall filter, FPC (Flexible PIC Concentrator) crash would be observed.
PR Number	**Synopsis**	**Category: Express PFE including evpn, vxlan**
1701636	Aggregated Ethernet interface member with vlan-id-list configured not forwarding traffic Product-Group=junos	On Junos QFX10002, QFX10008 and QFX10016 platforms, AE(aggregated-ethernet) interface member with vlan-id-list configured does not forward traffic thus leading to traffic loss.
1750468	L3VPN traffic destined for hosts learned over IRB/VXLAN will get dropped on QFX10K platforms Product-Group=junos	On QFX10K platforms in the DCI (Data Center Interconnect) scenario with EVPN-VXLAN traffic flow traversing over L3VPN, some packet drops will be observed when packets received over L3VPN with VPN label and destined to host learned over IRB/VXLAN tunnel.
PR Number	**Synopsis**	**Category: Enhanced Broadband Edge support for firewall**
1719427	The subscribers will be stuck in a terminated state when an FPC is taken offline Product-Group=junos	On MX platforms, If a Flexible PIC Concentrator (FPC) is taken offline while it has Broadband Edge (BBE) subscribers over it, due to timing issues a few subscribers state on the FPC may not get properly cleaned up and will be stuck in a terminated state. This can adversely affect subsequent subscriber logins which fail with an "orphaned filter" error.
PR Number	**Synopsis**	**Category: SRX4100/SRX4200 platform software**
1739559	SRX4100/4200 accepts the datapath-debug configuration although it does not support it Product-Group=junos	It is possible to set and commit the datapath-debug configuration on platforms SRX4100/SRX4200 although datapath debugging is not supported on those platforms. because of this unsupported configuration being accepted the RE (Routing Engine) load can go high and cause traffic outage. The workaround is to remove the datapath-debug configuration and perform a commit.
PR Number	**Synopsis**	**Category: Interface Information Display**
1636668	The management interface speed is reflected as 10G instead of 1G	On VMHost platforms, the management interface speed is displayed as 10G instead of 1G. There is no functionality

	Product-Group=junos	impact.
PR Number	**Synopsis**	**Category: ISIS routing protocol**
1746349	Traffic loss observed in SR-LDP stitch scenario when ECMP is enabled on PTX platforms Product-Group=junos	On PTX platforms, ISIS SR-LDP stitching using mapping server could result in traffic drops on some legs of an ECMP if there are more than 8 ECMP paths and not all paths are via the same neighbor node.
1752551	Traffic drop is seen if chained-composite-next-hop is turned on for Segment Routing Product-Group=junos	On all Junos and Junos Evolved platforms, Traffic drop is seen if chained-composite-next-hop is turned on for Segement Routing ISIS because backup path is programmed as a POP in Composite-next-hop (CNH) and Push in Forwarding-next-hop (FNH).
PR Number	**Synopsis**	**Category: jdhcpd daemon**
1714260	The DHCPv4 relay will send two option-82 to the server and the DHCP session will not be established Product-Group=junos	On all Junos and Junos OS Evolved platforms, when Dynamic Host Configuration Protocol (DHCPv4) Relay is configured with forward-only mode along with "trust-option-82", DHCP-relay should not add another option 82 to the packet sent to the DHCP server. The DHCP server upon receiving the packet with two option-82 will respond only with 1st header of option-82 which might get dropped by the relay, thus the packet is not forwarded to the DHCP client and the DHCP session won't get established.
1722082	DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only) Product-Group=junos	In EVPN VXLAN topology with DHCP stateless relay (forward-only) configured at layer 3 gateways, Jdhcpd broadcasts snooped unicast offer packets. That leads to the offer getting dropped on its way to the client and then the IP negotiation fails.
1731784	Dhcp security bindings may not happen when DHCP security is enabled on multiple vlans along with dhcp stateless relay Product-Group=junos	When DHCP security is enabled on multiple vlans along with dhcp stateless relay enabled at that time, dhcp security bindings may not happen.
1752804	Delay in getting IP through DHCP cause traffic loss Product-Group=junos	On all Junos and Junos Evolved platforms, DHCP IP negotiation will be delayed due to inform processing at Junos relay, when a client sends inform message to server and DHCP server doesn't respond with inform ack message and the client immediately does DORA to obtain IP.
PR Number	**Synopsis**	**Category: JFlow bug tracker for SRX platforms**
1716707	J-flow sends wrong IP in sampling records when NAT is configured for traffic along with input sampling Product-Group=junos	When NAT (Network Address Translation) is configured on interfaces along with sampling, the J-flow record will contain NAT'ed IP as opposed to the original IP.
1749830	SPC3 PIC crash Product-Group=junos	SPC3 PIC will crash when the SPU is in dedicated Cp mode "SPU Cp" and Jflow information is queried by vty command. This fix will prevent jflow related queries from vty when the SPC3 SPU is in dedicated CP mode and jflow is initialized on SPU ins this mode.

PR Number	Synopsis	Category: Issues related to Junos Kernel Debug Streaming Daemon (jkdsd
1734718	Junos OS: jkdsd crash due to multiple telemetry requests (CVE-2023-44188) Product-Group=junos	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in telemetry processing of Juniper Networks Junos OS allows a network-based authenticated attacker to flood the system with multiple telemetry requests, causing the Junos Kernel Debugging Streaming Daemon (jkdsd) process to crash, leading to a Denial of Service (DoS). Continued receipt and processing of telemetry requests will repeatedly crash the jkdsd process and sustain the Denial of Service (DoS) condition. Please refer to https://supportportal.juniper.net/JSA73152 for more information.

PR Number	Synopsis	Category: jl2tpd daemon
1720994	L2TP tunnels may time out if creation of bbe-smgd core dump takes a long time. Product-Group=junos	In a subscriber-management environment, L2TP tunnels may time out if bbe-smgd crashes with core dump if creation of the core dump takes longer than the effective L2TP timeout.

PR Number	Synopsis	Category: Adresses ALG issues found in JSF
1722877	Device crashed while processing H323 traffic in SRX and MX Product-Group=junos	The SRX Device and MX with MS-MPC and MX-SPC3 service cards, crashes due to a timing issue, while processing H323 traffic.
1728638	SIP ALG not working for SIP traffic with MIME header and traffic is dropped Product-Group=junos	On all MX and SRX platforms, SIP ALG (Session Initiation Protocol Application Layer Gateway) not working as SIP (Session Initiation Protocol) packets with MIME (Multipurpose Internet Mail Extensions) header causes traffic to be dropped.

PR Number	Synopsis	Category: Application aware Quality-of-Service
1720517	Junos OS and Junos OS Evolved: Multiple Vulnerabilities in CLI command (CVE-2023-44176) Product-Group=junos	A Stack-based Buffer Overflow vulnerability in the CLI command of Juniper Networks Junos OS allows a low privileged attacker to execute a specific CLI commands leading to Denial of Service. Repeated actions by the attacker will create a sustained Denial of Service (DoS) condition. Please refer to https://supportportal.juniper.net/JSA73140 for more information.

PR Number	Synopsis	Category: Flow Module
1613193	The flowd crashes on all SRX platforms Product-Group=junos	On all SRX platforms may encounter a core-dump during route lookup when PMI and vlan-tagging on interface are configured.
1624707	Flowd may core if route change or delete in PMI mode Product-Group=junos	Flowd may core if route change or delete and do IPSEC encap in PMI mode in SRX5K with SPC3 platform, please upgrade to version with this fix if using PMI mode in SRX5K with SPC3.
1664427	CPU utilization exceeds 95% which causes packets to drop and prevents new connections Product-Group=junos	On Junos non-5k SRX platform, the error message is generate because CPU (Central Processing Unit) utilization is over 95%. When the CPU over 95% on the system, packets are dropped and no new connections can be created until the CPU utilization is below 95% again. Traffic belonging to existing sessions is not

		affected.
1704623	Core dump will be seen when user is changing interface configuration Product-Group=junos	On SRX platforms with ALG (Application Layer Gateways) configured, frequent interface configuration changes will generate one or more core dumps after the flowd process crashes.
1708876	The IPv6 source-level fragmented SCTP packets passing through an IPSec tunnel will be dropped Product-Group=junos	On all SRX platforms, the IPv6 source-level fragmented Stream Control Transmission Protocol (SCTP) packets will be dropped when pass through an IPSec (Internet Protocol Security) tunnel.
1733819	The inet6 packet mode drops traffic significantly Product-Group=junos	On the SRX branch series, inet6 packet mode (packet-based) throughput drops significantly. Traffic will be fine until the CPU reaches 100% and random traffic will be dropped.
PR Number	**Synopsis**	**Category: all logging related bugs on srx platforms**
1716776	Security log missing space between timestamp and hostname Product-Group=junos	JunOS upgrade to the 22.2R3, 21.3R3-S3, 22.4R1, 21.4R3-S3, 22.3R2, 22.4R2, 21.2R3-S4 , 22.1R3 the security log space between the timestamps and site-name is removed Eg. 2023-08-14T12:04:31.273-07:00device_host-name RT_FLOW - RT_FLOW_SESSION_CREATE_LS [junos@2636.1.1.1.2.137 logical-system-name="JTAC-LSYS" source-address="10.10.10.10" source-port="29279" destination-address="10.10.30.20" destination-port="1603" connection-tag="0" service-name="icmp" nat-source-address="10.10.10.10" nat-source-port="29279" nat-destination-address="10.10.30.20" nat-destination-port="1603" nat-connection-tag="0" src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="1" policy-name="ONE" source-zone-name="JTAC-Trust" destination-zone-name="JTAC-dmz" session-id="3207" username="N/A" roles="N/A" packet-incoming-interface="ge-0/0/12.0" application="UNKNOWN" nested-application="UNKNOWN" encrypted="UNKNOWN" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A" tunnel-inspection="Off" tunnel-inspection-policy-set="root" source-tenant="N/A" destination-service="N/A"]
PR Number	**Synopsis**	**Category: Firewall Network Address Translation**
1712738	Some sessions will not be deleted when the NAT rule is deleted from the system Product-Group=junos	On all SRX platforms with NAT (Network Address Translation) configured, upon deleting a NAT rule the session associated with deleted rule continues to exist in the system, until the connection close initiated by the session. This is a rare timing issue.
PR Number	**Synopsis**	**Category: Firewall Policy**
1725567	Traffic impact is observed when the security policy is configured with a huge number of addresses and on addition/deletion of these policies Product-Group=junos	On SRX platforms configured with security policies, having a huge number (approx. 15K) of addresses and performing addition/deletion of such policies in short intervals of time might result in srxpfe process crash and hence, data path traffic gets impacted.

PR Number	Synopsis	Category: User Firewall related issues
1683420	SRX Branch models are unable to connect to domain controller on installing Microsoft KB update Product-Group=junos	On SRX300 series and SRX550M, when the User Identification feature is used with Active Directory, after the Domain Controller server installs updates related to Microsoft's KB article KB5004442, SRX is no longer able to connect to it. The PR1637548 did not fix this issue for these specific SRX platforms.
1701990	The user-id entries will not be synced with secondary node Product-Group=junos	On Junos platforms, user-id process doesn't work properly (user-id ?process also sync users primary and second node). As a result, active directory user-ip-mapping entries were not synced to the secondary node and due to that user connection will drop. When the issue happens, storage space eventually go full and the user may notice the issue at that time.
PR Number	**Synopsis**	**Category: IPSEC/IKE VPN**
1723674	Junos OS: Multiple Vulnerabilities in CLI command (CVE-2023-44178) Product-Group=junos	A Stack-based Buffer Overflow vulnerability in the CLI command of Juniper Networks Junos OS allows a low privileged attacker to execute a specific CLI commands leading to Denial of Service. Please refer to https://supportportal.juniper.net/JSA73140 for more information.
1745174	IPSEC VPN does not come up in NAT-T scenario Product-Group=junos	On all SRX platforms with IPSEC (Internet Protocol Security) VPN (Virtual Private Network) configured with main mode, if SRX is the VPN initiator and NAT-T (Network Address Translation-Traversal) is configured (which is by default), the IPsec VPN tunnel does not come up. This is a timing issue and occurs when a tunnel delete or rekey occurs.
PR Number	**Synopsis**	**Category: Security platform jweb support**
1735314	Editing security policy configuration via J-web is enabling "Exclude Selected" unexpectedly Product-Group=junos	On Junos platforms, when you cancel editing source/destination address in security policy using J-web, "Exclude selected" is unexpectedly enabled.
1735387	Junos OS: EX Series: A vulnerability in J-Web allows an unauthenticated attacker to upload arbitrary files (CVE-2023-36847) Product-Group=junos	A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on EX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity. With a specific request that doesn't require authentication an attacker is able to upload arbitrary files via J-Web, leading to a loss of integrity for a certain part of the file system, which may allow chaining to other vulnerabilities. For more information see https://kb.juniper.net/JSA72300
1735389	Junos OS: SRX Series: A vulnerability in J-Web allows an unauthenticated attacker to upload arbitrary files (CVE-2023-36846) Product-Group=junos	A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity. With a specific request that doesn't require authentication an attacker is able to upload arbitrary files via J-Web, leading to a loss of integrity for a certain part of the file system, which may allow chaining to other vulnerabilities. For more information see https://kb.juniper.net/JSA72300

1736942	Junos OS: EX and SRX Series: A PHP vulnerability in J-Web allows an unauthenticated to control important environment variables (CVE-2023-36845) Product-Group=junos	A PHP External Variable Modification vulnerability in J-Web of Juniper Networks Junos OS on EX Series and SRX Series allows an unauthenticated, network-based attacker to control certain, important environments variables. Utilizing a crafted request an attacker is able to modify a certain PHP environment variable leading to partial loss of integrity, which may allow chaining to other vulnerabilities. For more information see https://kb.juniper.net/JSA72300
PR Number	**Synopsis**	**Category: Junos Selective Update infrastructure**
1732878	The Junos Selective Upgrade (JSU) version is not removed post a major Junos upgrade/downgrade Product-Group=junos	There is no functional impact but the previously installed JSU will show up even though it is deleted during major upgrade. This PR will fix that issue. Workaround is to remove /packages/sets/active/junos-version file.
PR Number	**Synopsis**	**Category: Kernel MX virtual-chassis PRs**
1645671	Pseudo devices connected on ud and ut Interfaces stay down after hosting FPC was restarted Product-Group=junos	In MX-VC, if FPC enabling tunnel service is restarted, Pseudo devices connected on ud and ut Interfaces on the FPC stay down and never become up.
PR Number	**Synopsis**	**Category: Key Management Daemon**
1719216	A stale nat-long-route entry is present in the device causing incoming packets to be dropped Product-Group=junos	On all MX platforms with MS-MPC cards, When there is an active NAT (Network Address Translation) enabled IPSec (IP security) tunnel already present for a particular service-set, any change in the outside logical interface (IFL) becomes a stale entry in the forwarding table causing IKE (Internet Key Exchange) control and data traffic to drop.
PR Number	**Synopsis**	**Category: Layer 2 Control Module**
1720521	Junos OS and Junos OS Evolved: Multiple Vulnerabilities in CLI command (CVE-2023-44177) Product-Group=junos	A Stack-based Buffer Overflow vulnerability in the CLI command of Juniper Networks Junos and Junos EVO allows a low privileged attacker to execute a specific CLI commands leading to Denial of Service. Repeated actions by the attacker will create a sustained Denial of Service (DoS) condition. Please refer to https://supportportal.juniper.net/JSA73140 for more information.
1739975	Layer 2 traffic will be dropped on VSTP disabled interface Product-Group=junos	On Junos platforms, Whenever an interface is disabled under VSTP (VLAN Spanning Tre Protocol) configuration, the issue will be seen in the following cases. 1. When interface, IFBD (Interface Family Bridge Domain) and VSTP, configured via single commit. (In case of new configuration) 2. When VSTP configurations are present and chassisd restarts/device reboots, then issue will be seen. (During ifd delete and add, issue will be seen)
1745102	BPDU Protection with packet-action drop support on QFX10002-60C Product-Group=junos	BPDU Protection with packet-action drop support on QFX10002-60C
1763053	LLDP neighborship will not be formed on all Junos	On Junos and Junos OS Evolved platforms, LLDP (Link Layer

	devices Product-Group=junos	Discovery protocol) neighborship will not come up on local device if the local device is using Junos version lower than 22.3 (except 21.4R3-S2 and its subsequent service releases) and remote device is using Junos version 21.4R3-S2 and its subsequent service releases or version higher than 22.3.
PR Number	**Synopsis**	**Category: Layer2 forwarding on EX/NTF/PTX/QFX**
1723400	Unable to commit configs interface-mac-limit on sub-interfaces with vlan-tagging / flexible-vlan-tagging Product-Group=junos	On QFX10K platforms unable to configure interface-mac-limit on sub-interfaces with vlan-tagging / flexible-vlan-tagging.
PR Number	**Synopsis**	**Category: lacp protocol**
1609618	LACP Member interfaces might get stuck in out of sync state Product-Group=junos	When sync-reset feature is enabled on the device then few member interfaces might stay in out of sync state even when number of available child interfaces is greater than minimum-links configured for the Lag interface. This will affect the overall capacity of the lag interface.
PR Number	**Synopsis**	**Category: Label Distribution Protocol**
1635863	An rpd core is seen post graceful switchover Product-Group=junos	An rpd (Routing Protocol Daemon) crash is seen when dual transport LDP (Label distribution protocol) is configured along with NSR (Nonstop routing).
PR Number	**Synopsis**	**Category: Port-based link layer security services and protocols that a**
1726264	JSU installation fails when MACsec is configured Product-Group=junos	On Junos and Junos Evolved platforms with PPC based image (Example MX104), JSU (Junos Selective Update) package might not pass configuration validation when the MACsec (Media Access Control Security) configuration is present.
PR Number	**Synopsis**	**Category: Multiprotocol Label Switching**
1698889	The rpd process will crash when rpd is restarted Product-Group=junos	On all Junos and Junos OS Evolved platforms, when MPLS (Multiprotocol Label Switching) statistics is configured without LSP (Label-Switched Path) configuration, the rpd process will crash and impact the routing protocols. This leads to traffic disruption due to the loss of routing information.
PR Number	**Synopsis**	**Category: MX Timing software**
1653681	Junos OS: MX Series: In a PTP scenario a prolonged routing protocol churn can trigger an FPC reboot (CVE-2023-44199) Product-Group=junos	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA73165 for more information.
1715314	PTP statistics will not be visible after RE switchover. Product-Group=junos	On all Junos MX platforms with distributed PTP (Precision Time Protocol) timing feature, after RE (Routing Engine) switchover, PTP statistics will not be available. This is a display issue and

		very rarely seen.
1724254	On certain Junos MX platforms with SCB3 SyncE fails after enabling PTP Product-Group=junos	On Junos MX platforms having SCB3 (Switch Control Board), the SyncE (Synchronous Ethernet) can be stuck in "Clock_Aborted" state. This issue is seen in release 20.4R3 onwards when PTP (Precision Time Protocol) is operated in hybrid mode, the SyncE failure will hinder the operation of applications like G.8275.1 deployment will fail. There is a fix in 20.4R3-S4 with JSU (Juniper Selective Upgrade) J10.2. Below are the important notes to consider regarding the verification of the fix. --> JSU upgrade can be performed to replace the clksyncd with fix to address this issue. --> However, if the system is already in a problem state before the JSU upgrade, a one-time deactivate and activate of "protocols PTP" and "chassis synchronization" configuration is needed to recover from the current problem state after the JSU upgrade of clksyncd is performed.
1746541	MPC10E line card crashes when it reboots after FPC firmware upgrade Product-Group=junos	On MX240/MX480/MX960 platforms, if Precision time protocol (PTP) is configured, MPC10E line card crashes continuously after FPC firmware upgrade and when MPC10E line card is rebooted. Due to this issue, the clksyncd module also crashes.
1746984	PTP master feature will not work as expected Product-Group=junos	On MX240/MX480/MX960 platforms with SCBE3 (Enhanced Switch Control Board), PTP (Precision Time Protocol) master feature shall not work as expected. The qualified PTP CLK (8k) from RE (Routing Engine) will not propagate to other Line cards that are acting as Master to downstream nodes.
PR Number	**Synopsis**	**Category: OS IPv4/ARP/ICMPv4**
1722708	ksyncd core with dhcp subscribers Product-Group=junos	On all Junos platforms, in a very rare scenario, when subscriber-management and NSR is enabled, there could be a temporary transition state where one subscriber prefix has 2 nexthop referred. In that state if a deletion happened for that particular prefix, the nexthop deletion is successfully done one master RE but the deletion is failed on the backup RE. This eventually causes nh index inconsistency and then ksyncd core on backup RE. The fix is to make sure the deletion on the backup can be done successfully.
1752151	M/MX: Ksyncd cores are seen after performing Restart routing, with replication error Product-Group=junos	A receive only nexthop can have route change op, causing creation of a new DISCARD nh and moving route to the new nh. Refer arp_rcvonly_nh_addchg()/nd6_rcvonly_nh_addchg(). So, a route change can come to backup where the nexthop Id is different. Adding code to skip the nh index check in this case. Having VRRP config might hit a replication error on backup. Master RE will dump a live vmcore , but no functionality impact on master. Backup will recover on its own.
PR Number	**Synopsis**	**Category: FreeBSD Kernel Infrastructure**
1690892	After the VC is upgraded with NSSU (from/to 21.4R3)and rebooted again, the VCPs constantly flap and fail NSSU Product-Group=junos	When EX3400/EX2300 VC platforms are upgraded using NSSU (Nonstop Software Upgrade), and then after power cycling the VC (Virtual-Chassis), the VC gets unstable and the CPU usage of the new master might get too high.
1712855	Unicast packets are received on the management	On all platforms supporting em driver for their ethernet

	interface even though the destination MAC is not local Product-Group=junos	interface, promiscuous mode is enabled by default and hence traffic storm is noticed on the management interface.
PR Number	**Synopsis**	**Category: Kernel MPLS / Tag / P2MP Infrastructure**
1723145	Routing Engine initiated PING failed over MPLS interface Product-Group=junos	The RE-generated packets that have MTU size greater than the inet MTU size get dropped when going out on an interface with MPLS chain-composite-next-hop.
PR Number	**Synopsis**	**Category: TCP/UDP transport layer**
1694463	The vmcore crash observed in low memory conditions Product-Group=junos	On all Junos platforms, when there are low memory conditions vmcore crash is observed which impacts the traffic.
PR Number	**Synopsis**	**Category: OSPF routing protocol**
1737978	OSPFv3 using the VIP address on the IRB interface will not form adjacencies between peers Product-Group=junos	OSPFv3 may not form adjacencies on IRB interfaces with VRRP configuration.
PR Number	**Synopsis**	**Category: Express Chip L3 software**
1713279	Next-hop programming issue at PFE on Junos PTX and QFX10k platforms when the member of unilist is in hold state Product-Group=junos	On PTX Series routers and the QFX10000 line of switches, traffic going over unilist is dropped when unilist member goes from next-hop hold state to unicast/aggregate state.
1738541	Traffic drop observed when next-hop installation fails in a high-scale multicast/unicast scenario Product-Group=junos	On Junos PTX and QFX10K platforms, when the Flabel (Fabric Label) memory exhaustion occurs due to the scaled unicast/multicast next-hops and interface flapping i.e. downstream interfaces of multicast flapping, traffic drop is observed for next-hop installation failure in a high-scale multicast/unicast scenario.
PR Number	**Synopsis**	**Category: Protocol Independant Multicast**
1664211	The BSR information might not be flooded over NG-MVPN Product-Group=junos	On all Junos platforms, when the Protocol Independent Multicast (PIM) Bootstrap (BSR) packet comes over the Labeled Switch Interface (LSI), the BSR flooding/advertisement might not work and BSR information might not be flooded over the Next-Generation Multicast Virtual Private Network (NG-MVPN). This might impact the creation of the NG-MVPN.
1720708	Slow convergence of PIM joins causes temporary traffic loss with scaled downstream interfaces Product-Group=junos	On all Junos and Junos Evolved platforms with PIM (Protocol Independent Multicast), MVPN (Multicast Virtual Private Network) configured and when the number of downstream interfaces is more than three thousand, slow convergence of PIM joins is seen to take up more of the time and CPU, causing traffic loss for some time.
PR Number	**Synopsis**	**Category: PPPoE functional plugin for bbe-smgd**

1696221	The smgd (Enhanced Subscriber Management) crash is seen during creation/deletion of Interface-set in Subscriber management scenario Product-Group=junos	bbe-smgd process might crash with generating a coredump if any interface-set used for subscriber management has the length more than 12 characters.
1701739	Some PPPoE subscriber connection lost during RE switchover Product-Group=junos	On all Junos platforms, when rpd is busy on standby RE in deleting routes from previous subscriber termination, and followed by new subscriber login in master RE and switchover performed. Some PPPoE subscriber won't come up on new master RE.
PR Number	**Synopsis**	**Category: QFX access control list**
1730451	Error while configuring packet-forwarding-options on QFX5100 platforms Product-Group=junos	On QFX5100 platforms error occurs while configuring packet-forwarding-options
PR Number	**Synopsis**	**Category: QFX PFE Class of Services**
1641572	Traffic drop would be observed along with the error message 'Buffers are stuck on queue' when performing the OIR in the 100G QSFP interface Product-Group=junos	On QFX5110-32Q platforms, the traffic drop along with the error message "Buffers are stuck on queue" will be seen when the Online Insertion and Removal (OIR) is performed with 100G QSFPs on continuous ports 28,29,30,31 at the same time.
PR Number	**Synopsis**	**Category: DHCP related Issues**
1711525	DHCPv6 packets could not be forwarded if it contains the trailer or extra bytes out of the IP stack Product-Group=junos	On all Junos QFX5K and EX platforms with DHCPv6 (Dynamic Host Configuration Protocol) relay configuration, IPV6 (Internet Protocol) assignment could not take place as the DHCPv6 solicit packets containing extra bytes in DHCPv6 header trailer are not getting forwarded to the DHCP server.
1711644	QFX5000 Series and EX4000 Series: Denial of Service (DoS) on a large scale VLAN due to PFE hogging (CVE-2023-44191) Product-Group=junos	An Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA73155 for more information.
PR Number	**Synopsis**	**Category: QFX5K hostpath**
1721318	Error message is generated when DHCP packet is received via remote VTEP Product-Group=junos	The error message in VXLAN environment " d16-25 : %PFE-3: fpc0 Failed to get ifl for ifl index = 640". This can happen when the device receives DHCP packet via a remote VTEP and L3 interface (IRB) is not assigned on the egress interface. Even though there is no DHCP configuration, the packet injection happens and it fails to get IFL index as there is no IRB interface on the egress interface.
1723465	PFE crash is seen on Junos when file-logging is disabled Product-Group=junos	On Junos QFX5K platforms, when file-logging is enabled for ukern_trace handle and the logs are written continuously to the corresponding buffer due to a network issue, disabling file-logging for that handle will cause a PFE crash and will lead to a complete traffic loss.

PR Number	Synopsis	Category: QFX L2 PFE
1667069	Junos OS: QFX5000 series, EX2300, EX3400, EX4100, EX4400, and EX4600: Packet flooding will occur when IGMP traffic is sent to an isolated VLAN (CVE-2023-44203) Product-Group=junos	An Improper Check or Handling of Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent attacker to send specific traffic, which leads to packet flooding, resulting in a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA73169 for more information.
1705853	Tracking PR to add the null check for list_get_head if magic is NULL. Product-Group=junos	On all Junos platforms, as list_get_head function is called in multiple places in pfe we needed previous 3 functions on the stack which had called list_get_head, so we could debug why 'list_get_head list has bad magic' this error has occured.
1730076	Packets received on a port that is in "LACP Detached" state is getting forwarded Product-Group=junos	On all Junos EX46xx/QFX5k (except QFX5100) platforms, child links that are in LACP (Link Aggregation Control Protocol) detached state are up and accepting incoming traffic, expecting it to drop.
1736348	BFD session remains stuck in INIT state on certain QFX and EX platforms Product-Group=junos	On Junos QFX5120-48Y/EX4650-48Y/QFX5120-32C platforms, when the MAC (Media Access control) address corresponding to a next hop is updated, the BFD (Bidirectional Forwarding Detection) endpoints that are using this Next hop/egress is not picking up the updated MAC address and as result BFD session remains in INIT state and causes traffic impact.
1741316	The traffic drop is observed due to the MAC source address being learned from the wrong direction Product-Group=junos	On Junos EX4300/QFX5200/QFX5210 platforms with VXLAN (Virtual Extensible Local Area Network) enabled, when the ARP (Address Resolution Protocol) request is sent from the device, the MAC (Media Access Control) address is learned from the wrong direction which results in the traffic drop.
1759875	Generate an empty file whose name is secondary_vlan when executing RSI. Product-Group=junos	After executing "request support infomation | save " command, unexpected file will be generated.
PR Number	**Synopsis**	**Category: QFX L3 data-plane/forwarding**
1666260	Traffic is not restored when l2circuit configurations are deleted and added back on QFX5K Product-Group=junosvae	On Junos QFX5K platforms, flapping the Layer 2 circuit ports or removing and re-adding the configuration on the l2circuit ports, the re-configuration of the access side port fails and traffic ingressing or egressing out of that port gets dropped.
1704489	High CPU utilization causes a latency/slowness issue on QFX platforms Product-Group=junos	On QFX5110 and QFX5120 platforms, latency or slowness issue is observed when the traffic is passing through a layer 3 interface configured with just family inet/family inet6 due to unwarranted MAC lookup. This could lead to traffic loss on that interface.
1709664	BFD sessions flap on EX and QFX platforms Product-Group=junos	On all EX and QFX platforms, BFD(Bidirectional Forwarding Detection) sessions are flapped with VLAN configuration change on LAG interface.
1713133	The dcpfe crashes after restarting l2-learning process on QFX and EX series Junos platforms Product-Group=junos	The dcpfe process crash is observed on EX and QFX Junos platforms after restarting the l2-learning process when flex-hash is configured. It will be recovered automatically after the dcpfe

		restart
1714701	Traffic blackhole after reboot Product-Group=junos	On all Junos platforms, traffic drops observed when RH (Resilient-Hashing) is configured on a LAG (Link Aggregation Group) interface.
1724675	Traffic loss will be observed with vlan tagging and/or vlan normalisation in a specific design (using a looped cable) Product-Group=junos	Upon upgrade to Junos versions (junos:20.3R2, 20.3R3, 20.3X75-D20, 20.4R2, 21.1R1, 21.2R1), network connectivity is lost for traffic requiring vlan normalization and having DMAC one of the switch's MAC addresses. For example, incoming traffic has two vlans (S-vlan, C-vlan) ingressing on an interface and switch uses a looped link to provide routing via an IRB. --- (S-vlan|C-vlan) ---> SW_X --- C-vlan ---> SW_X_irb ARP and L2 learning occurs as expected but upon receiving the frame with DMAC of a local interface, switch takes a route lookup action instead of bridging and vlan normalization due to the frame having DMAC as the MAC of one of its interfaces. Hence, the traffic is not sent via looped cable to the L3 interface.
1725375	DCPFE process crash can be seen on all Junos EX and QFX5K platforms with MACSEC enabled Product-Group=junos	On all Junos platforms supporting MACSEC (Media Access Layer Security), the DCPFE (Dense Concentrator Packet Forwarding Engine) process might crash in a rare scenario when the configuration of MACSEC is deleted from the interface and the PFE is trying to access the memory location of the interface. The DCPFE process crash will lead to the FPC (Flexible PIC Concentrator) reboot but the system will self-recover.
1729101	dcpfe process core observed after restarting the l2-learning process with flex-hashing configuration Product-Group=junosvae	On Junos QFX (except QFX5210) and EX platforms, dcpfe core will be observed after the l2-learning process restarts when 'flex-hashing' is configured.
1732708	SNMP polling Timeout due to OID 1.3.6.1.2.1.31.1.1.1.10.514 (ifInOctets.514) Product-Group=junos	When trying to poll information via SNMP, the device stops reponding causing a SNMP timeout, the issue is due to sxe-0/0/0 private interface that is marked as public interfaces which causes it to query kernel for statistics.
1742763	Traffic drop will be observed after extended-vni-list configuration change with EVPN-VXLAN scenario Product-Group=junos	On Junos QFX5100/QFX5110/QFX5120/QFX5200/QFX5210/EX4100/EX4300-MP/EX4400-XX platforms having Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) configured if extended-vni-list configuration is deleted, the network interface is flapped and when extended-vni-list is added back due to this traffic using the Flood NH (BUM) on the device will be lost.
PR Number	**Synopsis**	**Category: QFX MPLS PFE**
1731291	Traffic for VLAN-id 2 gets dropped in Ethernet-CCC L2 Circuit on QFX5k/EX4650 platforms Product-Group=junos	On Junos QFX5k and EX4650 platforms traffic drop for VLAN (Virtual Local Area Network) having id 2 will be seen in the Ethernet-CCC (Circuit Cross Connect) L2 circuit. This happens because the VLAN-id is getting stripped at the egress PE (Provider Edge Router) hence causing a traffic drop at the CE (Customer Edge) Router.
1742364	Traffic dropped is observed in the MPLS LDP scenario when the peer device MAC address is changing Product-Group=junos	On Junos QFX5100 and EX4600 platforms when there is MAC (Media Access Control) change for the LDP (Label Distribution Protocol) neighbor and IP remains the same, the ARP (Address Resolution Protocol) update is proper but MPLS LDP may still use the stale MAC address of the neighbor. If there is any

		application/service such as MP-BGP using LDP as next-hop, all transit traffic pointing to the stale MAC address will be dropped.
PR Number	**Synopsis**	**Category: QFX EVPN / VxLAN**
1686539	The dcpfe process crashes on QFX5k and EX4k platforms Product-Group=junos	On QFX5k, EX4100, EX4300, EX4400, and EX4650 platforms, the dcpfe process crash will be seen when EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) is configured.
1712175	The dcpfe process crash is seen on QFX5k platforms due to stale vtep entry Product-Group=junos	On all QFX5000 platforms, with VXLAN (Virtual Extensible LAN) configured and due to a stale next hop entry of vtep (vxlan tunnel end point) interface, dcpfe (Dense Concentrator Packet Forwarding Engine) process crash was observed.
1729767	Junos OS: QFX5000 Series, EX4600 Series: In a VxLAN scenario an adjacent attacker within the VxLAN sending genuine packets may cause a DMA memory leak to occur. (CVE-2023-44183) Product-Group=junos	An Improper Input Validation vulnerability in the VxLAN packet forwarding engine (PFE) of Juniper Networks Junos OS on QFX5000 Series, EX4600 Series devices allows an unauthenticated, adjacent attacker, sending two or more genuine packets in the same VxLAN topology to possibly cause a DMA memory leak to occur under various specific operational conditions.Please refer to https://supportportal.juniper.net/JSA73148 for more information.
1730771	Traffic is impacted due to high CPU and dcpfe/fxpc crash (in some cases) in EVPN-VXLAN scenario Product-Group=junos	On Junos QFX5k and EX platforms, a high CPU and dcpfe/fxpc crash (in some cases) is seen in the EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) scenario.
1731583	Traffic drops when any of the VXLAN VLAN is deleted Product-Group=junos	On Junos QFX5100, EX4600, QFX5200 and QFX5210 platforms whenever any of the EVPN (Ethernet Virtual Private network) - VXLAN (Virtual Extensible LAN) VLAN (Virtual Local Area Network) is removed from the interface having multiple VXLAN VLANs configured, then the VXLAN traffic for all the other VLANs within that interface is seen to get dropped.
PR Number	**Synopsis**	**Category: QFX10008/16 QFX10002 Ultimat/Elit platform related issues -**
1734734	Online SIBs will go down due to a faulty SIB that triggers spmbpfe crash Product-Group=junos	On all the QFX10000 line of switches and PTX Series routers running Junos OS, due to initialization failure of a faulty Switch Interface Board (SIB) in the device, the Switch Processor Mezzanine Board (SPMB) status process, also known as the spmbpfe process, crashes and online SIBs go down.
1742186	SPMB process will crash and PICs will not come online Product-Group=junos	On the QFX10000 line of switches running Junos OS, due to initialization failure of a faulty Switch Interface Board (SIB) in the device, the Switch Processor Mezzanine Board (SPMB) status process, also known as the spmbpfe process, crashes and online SIBs go down. Traffic cannot flow through the line card when this happens.
PR Number	**Synopsis**	**Category: QFX5100 Interface related issues**
1688023	The LLDP output packets are not transmitting on the em0 interface of Junos and Junos OS Evolved platforms Product-Group=junos	On Junos and Junos OS Evolved platforms, if a management Ethernet interface(em0) has an inet or inet6 family configured and "delete interfaces em0" is issued, the Link Layer Discovery Protocol (LLDP) output packets will stop transmitting, causing

		the LLDP neighborship to remain down in peer router.
PR Number	**Synopsis**	**Category: QFX5100 Virtual Chassis**
1718062	VCP ports on 10G not coming up after reboot Product-Group=junos	In a VC of QFX5100-24Q with an expansion module EX4600-EM-8F, if VC is formed on 10G ports then after the reboot of VC, the 10G connections will be lost and the line card will show as not present. This will impact traffic on the 10G ports after connection is lost.
1729067	Traffic loss will be observed due to CRC errors with QSFP+-40G-ACU10M plugged Product-Group=junos	On QFX5K platforms with QSFP+-40G-ACU10M and Virtual Chassis configured, traffic loss will be observed due to CRC (Cyclic redundancy check) errors.
1746788	[QFX5K]When RSI(request support information) is executed in the VC configuration, some errors output Product-Group=junos	On QFX5K platform, "request pfe execute ... target fpc" in RSI is always executed on master role in the VC configuration.
PR Number	**Synopsis**	**Category: QFX5200/5110/5120/5210 Platfom issues**
1710952	No alarm is raised when PSU is inserted with different airflow directions Product-Group=junosvae	On QFX5100/QFX5110/QFX5120/QFX5200 platforms, no alarm would be raised even though inserted PSU module which has a different airflow.
1720884	Interface with QSFP+-40G-CU50CM will be down Product-Group=junosvae	The interface will be down on EX and QFX platforms with QSFP+-40G-CU50CM (740-044512) resulting in traffic loss. In the VCP (Virtual Chassis port) scenario if connected with QSFP+-40G-CU50CM it does not come up and break the VC (Virtual Chassis) environment when upgrading or rebooting the device.
1725116	Sometimes 100G link will go down and will remain down Product-Group=junosvae	On the Junos QFX5200 platform, sometimes 100G link will go down and will remain down
PR Number	**Synopsis**	**Category: QFX5K Timing software**
1683308	The dcpfe crash seen with PTP configuration on Junos platforms supporting boundary clock Product-Group=junos	On Junos platforms supporting boundary clock, dcpfe crash is seen with Precision Time Protocol (PTP) configuration. This is due to a timing issue between the periodic poll and stream addition.
PR Number	**Synopsis**	**Category: RPD infrastructure issues related to NSR, GRES, switchover,**
1727957	The traffic drop is observed during the Graceful restart on Junos and Junos Evolved platforms Product-Group=junos	On all Junos and Junos Evolved platforms, during the time of Graceful restart(GR), the routes in the Multiprotocol Label Switching(mpls).0 table will be updated even when the routing protocols are in the process of re-convergence and have not yet come out of GR. This causes inaccurate routes in the routing table and traffic drop is observed during GR.
PR Number	**Synopsis**	**Category: KRT Queue issues within RPD**

1721032	Local route is not added in the secondary FIB on all Junos SRX platforms and routes will be permanently stuck in KRT queue Product-Group=junos	On all Junos SRX platforms when ST (Secure-Tunnel) interface with P2MP (Point-to-Multipoint) is configured and interface routes are leaked via RIB-group (Routing Information Base), local route of the ST interface will not be leaked into forwarding-table of the secondary-RIB and it will be stuck in the KRT (Kernel Routing Table) queue.
PR Number	**Synopsis**	**Category: RPD route tables, resolver, routing instances, static routes**
1746439	Route-distinguisher change leads to the route being present in rpd, but not installed in kernel/PFE Product-Group=junos	On Junos and Junos Evolved platforms, traffic impact will be observed when route-distinguisher change is performed for which route will be present in rpd, but not installed in kernel/PFE. This issue happens when the aggregate route is configured.
PR Number	**Synopsis**	**Category: Resource Reservation Protocol**
1703424	Pathtear message is not forwarded by PLR to merge point which is causing data plane blackholing Product-Group=junos	On all Junos and Junos OS Evolved platforms, the PLR (point of local repair) is not sending the pathtear message when the merge point supports the enhanced FRR while the route reaching the neighbor is using a shortcut route under MVPN (Multicast Virtual Private Network) configured scenario.
PR Number	**Synopsis**	**Category: SW PRs for SCBE3 chassisd**
1667226	The hyper-mode might be set incorrectly after power cycle on MX platforms Product-Group=junos	The hyper-mode can be set incorrectly after power cycle on MX platforms when either BBE and/or MX VC is configured and hyper-mode is not configured.
PR Number	**Synopsis**	**Category: Bug and Review Tracking for Segment routing traffic eng**
1709557	The telemetry sensor will not be created for PCE initiated SRTE Product-Group=junos	On all Junos and Junos Evolved platforms, for PCE(Per-Path Computation Element) Initiated (provisioned) uncolored-SRTE(Segment Routing Traffic Engineering) tunnels, per-source per-segment-list telemetry sensors are not created.
1720031	The rpd process crash will be observed while creating/updating the PCEP tunnel Product-Group=junos	On Junos and Junos OS Evolved platforms, when SR (Segment Routing) PCEP (Path Computation Element Protocol) provisional tunnel is configured along with the template but the template has delegation configured, then the PCEP update message received for creating/updating tunnels is causing the rpd process crash and tunnel creation/update will fail for PCEP provisional tunnel.
1737119	The traffic blackhole will be observed when the SRTE shortcut is configured Product-Group=junos	On Junos platforms, when the MPLS (Multiprotocol Label Switching) packet reaches the destination router, it will have a label that is unknown to the destination router due to a label POP operation miss at the ingress router resulting in the traffic black hole in the scenario SR-MPLS (Segment Routing With Multiprotocol Label Switching) + traffic engineering shortcut is configured.
PR Number	**Synopsis**	**Category: SRX Argon module**

1737442	Intermittent core-dumps is received when SMB protocol is enabled on AAMW policy and PFE memory is exhausted Product-Group=junos	On SRX platforms, When Server Message Block(SMB) protocol is enabled on advanced anti-malware(AAMW) policy and PFE memory is exhausted in that condition, SMB and SMTP is calling the same fallback API results high memory utilization. There are two types of cores is generated one is from AAMW plugin and the other is from DNS plugin. Both of them are because memory is exhausted and these high memory utilization can cause PFE process crash which results network outage for a while.
1738656	Traffic drop caused by PFE memory leak on SRX platforms Product-Group=junos	On Junos SRX platforms enrolled into ATP (Advanced Threat Prevention) cloud, memory leak is observed in the PFE (Packet Forwarding Engine) while deletion of few of the signatures which have no hash value. This memory leak results in traffic loss.
PR Number	**Synopsis**	**Category: security-intelligence feature on SRX**
1696110	Junos OS: SRX Series: The PFE will crash on receiving malformed SSL traffic when ATP is enabled (CVE-2023-36843) Product-Group=junos	An Improper Handling of Inconsistent Special Elements vulnerability in the Junos Services Framework (jsf) module of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a crash in the Packet Forwarding Engine (PFE) and thereby resulting in a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA73174 for more information.
PR Number	**Synopsis**	**Category: SRX branch platforms**
1658968	The DNS information is getting lost when IPCP flaps Product-Group=junos	On all SRX-branch series platforms working as a PPPoE (Point-to-Point Protocol over Ethernet) client and a DHCP (Dynamic Host Configuration Protocol) server, DNS (Domain Name System) information is getting lost, for which the DHCP client won't receive DHCP information and DNS packets will not get resolved to result in the packet drops. This issue happens when the IPCP (Internet Protocol Control Protocol) source address is not getting copied and IPCP is getting flapped due to the interface (DHCP interface) being flapped.
1709013	Kernel panic on Junos (FreeBSD) platforms Product-Group=junos	On Junos (FreeBSD) platforms, kernel panic was seen.
1713759	Continuous vmcores observed on the secondary node when committing the "set system management-instance" command Product-Group=junos	On Junos SRX3xx series platforms, when the "set system management-instance" command is committed on the secondary node, continuous vmcores are observed on primary and secondary nodes. No recovery action is needed for the primary node and the secondary node of the cluster reboots automatically to recover from the error. The cluster redundancy is not restored until the management-instance knob is removed using the "delete system management-instance".
1714620	High latency will be observed while pinging to peer device Product-Group=junos	On Branch SRX Platforms, The delay will be observed while pinging to peer device due to high latency when VLAN(Virtual Local Area Network) tagged DHCP(Dynamic Host Configuration Protocol) packets arrive at IRB (Integrated Routing and Bridging) interface.
1715247	Interface speed stays 100Mbps when removing speed and duplex command separately	On SRX branch series, when the interface speed is set to 100Mbps and the link-mode is set to full-duplex, the interface

	Product-Group=junos	speed remains at 100Mbps even the speed and duplex commands are removed separately.
1719108	OAM not working with flexible-vlan-tagging Product-Group=junos	OAM is not working when flexible-vlan-tagging is enabled
1768050	SRX3XX : ARP is not getting resolved Product-Group=junos	On SRX300 series devices, ARP resolution does not work for BGP sessions. This issue only applies to Junos releases 21.4R3-S5 and 22.1R3-S4.
PR Number	**Synopsis**	**Category: SRX5XX platform**
1620982	8-Port Gigabit Ethernet SFP XPIM not passing traffic after software upgrade Product-Group=junos	On SRX550 platform, after doing a software upgrade, 8-Port Gigabit Ethernet SFP XPIM is not passing traffic
PR Number	**Synopsis**	**Category: Stout cards (MPC7, MPC8, MPC9) microkernel issues**
1727427	FPC crash observed when the ASIC usage is high Product-Group=junos	On platforms with MS-MPC/MPC1/2/3/4/5/6/7/8/9/JNP10K-LC2101/JNP10003-LC2103/JNP10K-LC480 line cards and EX9200/EX9204/EX9208/EX9214/EX9251/EX9253 series devices, route churn (add or deletes) when the ASIC usage crosses a threshold (ASIC usage is high) which leads to a FPC crash.
PR Number	**Synopsis**	**Category: MX10002 Platform SW - Platform s/w defects**
1721714	BFD session failed when configured on the loopback sub interface Product-Group=junosvae	On the MX10003 and MX304 platforms, BFD (Bidirectional Forward Detection) session failed to come up when configured on the loopback sub interface.
PR Number	**Synopsis**	**Category: SRX-1RU platfom related protocol, QoS, filtering features et**
1729284	L2 channel error counter increases when unknown family packets received by interfaces Product-Group=junos	On SRX4600 and SRX5K platforms, the L2 channel error counter will increase when some unknown family packets received by interfaces.
1737721	Junos OS installation using USB can fail on SRX4600 Product-Group=junosvae	On SRX4600 platforms, Junos OS installation using USB can fail due to slow USB detection.
PR Number	**Synopsis**	**Category: ZT/YT pfe qos software issues**
1715149	DSCP field in IPv4 header is incorrectly re-written Product-Group=junos	On Junos platforms that support MPC10/MPC11/LC9600 line cards, whenever there is a rewrite rule configured to rewrite the DSCP bits on transit router in core network, packet loss are observed in the destination due to incorrectly re-written DSCP field in IPv4 header.
PR Number	**Synopsis**	**Category: ZT/YT pfe firewall software**
1726733	Traffic drops with percent policer attached using list Product-Group=junos	On Junos EX92xx, MX304 and MX series platforms with MPC10, MPC11 and LC9600, traffic drop will happen with the attachment of family filter configured with percent policer

		(bandwidth-percent) via input-list/output-list.
1738548	DHCP offer is dropped at MX and specific EX platforms when an lt interface is used as the transport Product-Group=junos	On MX and EX92_XX platforms, the DHCP offer will be dropped when LT interface is used to reach the DHCP server. DHCP relay will not work as expected due to this issue.
PR Number	**Synopsis**	**Category: ZT/YT pfe l3 forwarding issues**
1719763	L2 circuit connection not working with flow-label knob Product-Group=junos	On Junos MX platforms, packet drop is seen in Layer 2 circuit when flow-label is enabled along with control-word and the egress Provider Edge (PE) core facing interface is on MPC10E/11E/LC9600/MX304-LMIC16. Certain flows will get punted to RE (Routing Engine) instead of getting forwarded.
PR Number	**Synopsis**	**Category: Issues related to broadband edge apps (PPP, DHCP) on Trio ch**
1718595	Subscribers disruption is seen on the AE interface after the "disable-pfe" action Product-Group=junos	On all MX platforms with MPC7/8/9/LC2101/LC2103 line cards, when a "disable-pfe" action is executed for major cmerrors, there will be improper flagging of timeouts and incorrect logging out for all subscribers in scenarios where an AE(Aggregated Ethernet) interface is present on the disabled PFE(Packet Forwarding Engine).
1722945	PADT response will not be sent for an incoming PPPoE/PPP data Packet from an unknown session ID Product-Group=junos	On all MX platforms with line cards before MPC10, when Broadband Network Gateway (BNG) switchover occurs, the new master does not send PPPoE Active Discovery Termination (PADT) packet for an unknown session if the incoming packet is PPPoE/PPP data packet and thus the existing subscribers does not come up on this router.
PR Number	**Synopsis**	**Category: Trio pfe qos software**
1700860	The egress rewrite-rule might not work as expected for traffic entering the AE interface Product-Group=junos	On all MX platforms, if the loss-priority is not explicitly configured on the AE (Aggregated Ethernet) interface, the default classifier is applied, but the loss-priority is not properly set at certain DSCP (Differentiated Services Code Point) code points and the rewrite does not execute as expected.
1714429	The DEI bit will not be copied in the inner VLAN tag although the incoming traffic has the DEI bit set Product-Group=junos	On all Junos platforms, there might be a service impact if the DEI (Drop eligible indicator) bit is used to decide if the packet needs to be dropped or not as the DEI bit will not be copied in the inner VLAN tag although the incoming traffic has the DEI bit set. The issue will happen when the dot1p (IEEE 802.1p) rewrite is bound to the egress interface with inner and outer tag options in the P2P (Point-to-Point) L2VPN (Layer 2 Virtual Private Network) environment.
PR Number	**Synopsis**	**Category: Trio pfe stateless firewall software**
1682164	Traffic drop is seen after configuring fast-lookup-filter Product-Group=junos	On MX platforms with specific line cards, when fast-lookup-filter (FLT) is used on a highly scaled device, a packet processing loop in PPC will corrupt the internal next-hop lookup, causing a traffic drop.

1737615	MPC1 to MPC13E/LC2101,LC2103,LC480/T4000-FPC5/MPC built-in Trio based line card reboots when subscriber management services are configured Product-Group=junos	When Junos EX, MX, SRX, T platforms with Modular Port Concentrators from MPC1 to MPC13E/LC2101,LC2103,LC480/T4000-FPC5/MPC built-in Trio based line cards are configured with subscriber management services with interface name that exceeds 19 characters, it leads to line card reboot causing service impact.
PR Number	**Synopsis**	**Category: Trio pfe bridging, learning, stp, oam, irb software**
1727049	Multiple CFM sessions are down when vlan rewrite feature is configured on AE interfaces Product-Group=junos	On MX platforms, in Aggregate Ethernet (AE) interfaces having the member links in MPC1 to MPC9 line cards with Circuit Cross-Connect (CCC) when Maintenance Association End Point(MEP) is configured a new Virtual Local Area Network (VLAN) rewrite feature has been added before punting the Cross-connect Continuity Check Message (CCM) packets. This feature is derived from the AE member interfaces where the Packet Forwarding Engine (PFE) instance of the member is wrongly updated causing the Connectivity Fault Management (CFM) sessions down.
PR Number	**Synopsis**	**Category: Trio pfe l3 forwarding issues**
1707742	Junos OS: MX Series: Receipt of malformed TCP traffic will cause a Denial of Service (CVE-2023-36841) Product-Group=junos	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated network-based attacker to cause an infinite loop, resulting in a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA73172 for more information.
PR Number	**Synopsis**	**Category: XMCHIP Related SW Issues**
1724841	Memory initialization and scrub operation using PFE's fails Product-Group=junos	On MPC5/6/7/8/9 line cards, the memory initialization/scrub operation using PFE's (Packet Forwarding Engine) may fail in very rarely scenario. If memory scrub at line card initialization fails we may see initialization errors and a large number of PFE traps. Partial to full service impact depending on which event failed.
PR Number	**Synopsis**	**Category: Junos Automation, Commit/Op/Event and SLAX**
1717425	Junos platform device unable to commit configuration in recovery mode Product-Group=junos	On all Junos platforms where snapshot is supported, when a device is rebooted from recovery mode it fails to commit configuration due to problems with slax import and device might go into amnesiac mode due commit fail.
PR Number	**Synopsis**	**Category: Configuration mgmt, ffp, load-action, commit processing**
1562848	The mustd process may crash on all platforms Product-Group=junos	With a large-scale configuration, in rare cases, the mustd may crash. The mustd process, which is responsible for configuration constraint checks, might crash on commit, leading to commit failure.
1659783	The configuration might roll back after performing	On all Junos OS and Junos OS Evolved platforms, the

	"commit confirmed" and then reboot Product-Group=junos	configuration might roll back after performing "commit confirmed" and then a reboot.
1663590	Commit failure might be observed on reactivation or commit of specific configurations after the upgrade of the device Product-Group=junos	On all Junos and Junos Evolved platforms, reactivation or commit of specific configurations fails after the upgrade of the device.
PR Number	**Synopsis**	**Category: UI Infrastructure - mgd, DAX API, DDL/ODL**
1638847	The mustd process crash might be observed with persist-group-inheritance Product-Group=junos	On all Junos and Junos Evolved platforms configured with persist-group-inheritance, which is enabled by default from 19.4R3 onwards, might lead to mustd process crash in highly scaled configuration.
1648744	JDI-RCT:M/Mx: While removing VRRP configs and adding them back, mgd process stuck at 100% and router hangs forever. Product-Group=junos	While removing VRRP configs and adding them back, the mgd process stuck at 100% and the router hangs forever.
1693630	In JUNOS EVO "show | display inheritance" does not work correctly for LSPs with whitespace in the name Product-Group=junos	An LSP with whitespace in the name does not display correctly when viewing the configuration using 'show | display inheritance'
1706285	Junos OS and Junos OS Evolved: High CPU load due to specific NETCONF command (CVE-2023-44184) Product-Group=junos	An Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in the management daemon (mgd) process of Juniper Networks Junos OS and Junos OS Evolved allows a network-based authenticated low-privileged attacker, by executing a specific command via NETCONF, to cause a CPU Denial of Service to the device's control plane. Please refer to https://supportportal.juniper.net/JSA73147 for more information.
1730336	The rpd crashes and the commit operation fails while pushing a large configuration with the "extend-size" knob enabled Product-Group=junos	On all Junos platforms, when the 'extend-size' knob is configured and a scaled configuration is committed, the rpd daemon crash is seen and the commit operation fails.
1740289	The 'load replace' operation might result in mustd and mgd crash Product-Group=junos	On Junos and Junos Evolved platforms with apply-group configured, mustd and mgd crash might be observed when the 'load replace' operation is performed due to which all the apply-groups will get deleted internally, and respective hierarchies will not be notified.
1745565	The mgd process crash is observed when 'show' is executed from the configuration mode Product-Group=junos	On all Junos platforms, when 'show' is executed from the configuration mode, a mgd process crash is observed which has no functionality impact.
PR Number	**Synopsis**	**Category: web filterig issues**
1715260	utmd core has seen at commit when *.* or *.*.* is configured at url-pattern Product-Group=junos	When url-pattern contains '*.*' or '*.*.*', utmd core is generated and commit fails .
PR Number	**Synopsis**	**Category: Junos Fusion Satellite Device Infrastructure**

1682680	The Junos Fusion Satellite device will be stuck in the SyncWait state Product-Group=junos	On Junos MX, EX, and QFX platforms, post rebooting the device the Junos Fusion Satellite devices are trying to generate the ssh keys before clearing the old keys. The Satellite devices will not be responsive as they are stuck in the SyncWait state leading to traffic loss.
PR Number	**Synopsis**	**Category: For GPRS security features on highend SRX series**
1750988	SRX dropping GTP ChangeNotificationRequest messages due to "Non-zero TID/TEID Product-Group=junos	The change notification request and response gtpv2 messages received with non-zero TEID are being dropped. This might have been in agreement with previous ETSI requirement. But as per latest releases, such messages with non-zero TEID also shall be passed and not dropped.
PR Number	**Synopsis**	**Category: Virtual Router Redundancy Protocol**
1697394	VRRP Master session on AE ifl having child links on Satellite Device stops transmission post GRES Product-Group=junos	On Junos Fusion Aggregation Device platforms, when the VRRP (Virtual Router Redundancy Protocol) interface is configured on IRB (Integrated Routing and Bridging) with underlying L2 interface on Satellite Device post GRES (graceful Routing Engine switchover) VRRP Master stops transmission of VRRP PDU (Protocol Data Unit) resulting in VRRP Master/Master state.
1720943	Issue in VRRP inline adjacency whenever a master router uplink goes down on MX platforms Product-Group=junos	On all Junos MX platforms, when "set protocols vrrp delegate-processing" knob is enabled in Virtual Router Redundancy Protocol (VRRP) protocol and VRRP track is also enabled for uplink interfaces in that scenario if the master router uplink fails and the master priority remains higher than the backup router even after the master router uplink failure, this results in an issue with VRRP inline adjacency.
PR Number	**Synopsis**	**Category: usf url filtering related issue**
1737670	URL-Filtering few HTTP sites are getting bypassed and redirect is not happening Product-Group=junos	On Junos MX series platforms with service card (SPC3, MS-MPC and MS-MIC), when the contents in the url-filter-database file are in upper case, the URL (Uniform Resource Locator) filtering fails to filter those HTTP (Hypertext Transfer Protocol) URIs (Uniform Resource Identifier) which are meant to be redirected.
1751860	Service PIC enabled with url-filtering may crash and gets into booting loop Product-Group=junos	On MX platforms, with service cards running url-filtering plug-in, when the domain-names are resolved with more than 10 IPv6 or IPv4 addresses, may results in service PIC crash.
PR Number	**Synopsis**	**Category: usf flow and datapath issue on SPC3**
1750634	Traffic transfer is impacted for SPC3 CPU cores over the affected PCIe bus during SPC3 card bootup Product-Group=junos	On MX and SRX platforms with SPC3 card, SPC3 (Services Processing Card 3) CPU cores over the affected PCIe (Peripheral Component Interconnect) bus (7 CPU cores) will not transfer any traffic during SPC3 card bootup due to incorrect register settings.
PR Number	**Synopsis**	**Category: usf logging and reporting function related issues**
1744563	[USF - SPC3 - LOGGING] "log-tag" is not populated in	Sometimes, the log-tag within a stream is not used in syslog

	the cgnat syslogs intermittently Product-Group=junos	generation.
PR Number	**Synopsis**	**Category: usf nat related issues**
1598382	The TCP keepalive does not reach host on the private Network Product-Group=junos	On all MX platforms with SPC3 cards where tcp-tickle knob is enabled under services-options in DS-lite (Dual-Stack lite) with NAT scenario , TCP keepalive sent by AFTR (Address Family Transition Router) will not be properly encapsulated by IPv6 addresses.
1729801	Traffic drops are observed on MX Platform configured with PCP mapping along with NAT Product-Group=junos	On all MX platforms with SPC3 cards and PCP (Port Control Protocol) with NAT (Network Address Translation) configured, the PCP client should renew the mapping before its expiry time to keep the PCP mapping always active. The sessions are not refreshed with the received PCP mapping refresh. The issue is seen if the traffic from outside the network (public network) toward B4 (softwire initiator) was suspended for sometime. When traffic started again toward B4 from outside the network, it will be dropped and service will be impacted.

21.3R3-S5 - List of Known issues

PR Number	Synopsis	Category: Daily JUNOS build failures - automated builder use only
1691209	Use latest os-package when upgrading Product-Group=junos	Upgrade to 22.3R1 while using os-package published between July 2022 and November 2022 may incorrectly link os-libs package *Resolved In:* junos:21.2R3-S4 junos:21.3R3-S3 junos:21.4R3-S2 junos:22.1R3-S1 junos:22.2R2-S1 junos:22.2R3 junos:22.3R1-S2 junos:22.3R2 junos:22.4R1 junos:22.4R2
PR Number	**Synopsis**	**Category: EX4300 PFE**
1610408	The pfex core might be seen after the device is running for a while Product-Group=junosvae	In a Virtual chassis. the pfex core could be seen after the device is running for a while and due to PFE restart, VC may split and drop packets in forwarding plane. There is no specific time frame as well as any trigger. *Resolved In:* junos:19.4R3-S6 junos:20.1R3-S2 junos:20.2R3-S3 junos:20.3R3-S1 junos:20.4R3 junos:21.1R3 junos:21.2R2 junos:21.3R1 junos:21.4R1
PR Number	**Synopsis**	**Category: EX4300 Platform**
1733339	On EX4300-VC, the PFE might crash if a QSFP is inserted or removed when the CPU is stressed Product-Group=junos	On EX4300-VC, the Online Insertion and Removal (OIR) of Quad Small Form-factor Pluggable (QSFP) may result in a PFE crash under near-zero idle CPU conditions. *Resolved In:* junos:20.4R3-S8 junos:21.4R3-S4
1747126	On EX4300-VC,	On EX4300 VC setup, "qsfp_tk_read_mem_page: Rear QSFP+ PIC failed to select addr

	qsfp_tk_read_mem_page messages might be seen after an upgrade Product-Group=junos	127 err 1000" messages may be seen intermittently. There is no functionality impact for these error messages *Resolved In:*
PR Number	**Synopsis**	**Category: EX4300 Layer 2 implementation**
1739730	In EVPN-VXLAN scenario DHCP does not work for clients connected on the dot1x port Product-Group=junos	On EX4300-48MP, in case of dot1x EVPN-VXLAN dynamic VLAN due to a HW setting which is used to assign VLAN to the authenticated dynamic VLAN, causes the DHCP offer to get tagged. *Resolved In:* junos:21.2R3-S7 junos:21.4R3-S4 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R2-S2 junos:22.3R3-S1 junos:22.4R2-S2 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: EX2300/3400 PFE**
1706845	Layer 3 forwarding issues for IRB Product-Group=junos	On EX2300, EX3400, EX4400, EX4100 and EX4300-MP platforms, when master FPC with mac-persistence-timer configured on a virtual chassis switch is halted, it leads to layer 3 (l3) forwarding issues for the integrated routing and bridging (IRB). *Resolved In:* junos:20.4R3-S7 junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S3 junos:21.4R3-S4 junos:22.1R3-S2 junos:22.2R3 junos:22.2R3-S1 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.2R1
PR Number	**Synopsis**	**Category: EX2300/3400 platform**
PR Number	**Synopsis**	**Category: SRX DNS DGA and tunneling related**
1727122	Nstraced process is running high on the primary node after the Junos upgrade Product-Group=junos	On all Junos SRX/vSRX platforms, nstraced process spikes to 100% usage after upgrading to Junos version 21.4R3-S2 or any later releases without having any traces/debugs explicitly configured in the RE (Routing Engine) or PFE (Packet forwarding Engine) of the device. *Resolved In:* junos:21.4R3-S5 junos:22.1R3-S3 junos:22.2R3-S3 junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: SRX 5K SPC3 FPGAs**
1671649	Traffic loss may be seen due to SPC3's packets getting stuck Product-Group=junos	On Junos MX960, MX480 and SRX5000 series platforms with SPC3 card, Flowd restart or PIC (Physical Interface Card) going offline/online may cause SPC3's sending of packets to get stuck. *Resolved In:* 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:21.1R3-S4 junos:21.2R3-S3 junos:21.3R3-S3 junos:21.4R3-S1 junos:22.1R2-S1 junos:22.1R3 junos:22.2R1-S2 junos:22.2R2 junos:22.2R3 junos:22.3R1-S1 junos:22.3R2 junos:22.4R1 junos:23.1R1
PR Number	**Synopsis**	**Category: Fireall support for ACX**
1737999	Transit VPN traffic towards local CE failed in ARP resolution due to VRF lo0.x RE filter in	On ACX1K/2K platforms, when a lo0.x filter is configured under a vrf type routing-instance, any IPv4 transit traffic that makes ARP request to generate to the CE-facing interfaces will fail in ARP resolution due to the ARP request packets are

	place Product-Group=junos	discard by lo0.x filter if no specific term to accept the IPv4 packets *Resolved In:* junos:21.2R3-S6
PR Number	**Synopsis**	**Category: ACX L2 related features**
1720141	Devices stop passing VPLS traffic following a link flap causing LSP switchover Product-Group=junosvae	On ACX5048 and ACX5096 acting as PE (Provider End) routers, when the VPLS (Virtual Private LAN Service) gets switched multiple times between the primary path and backup path after some time programming fails and the software starts throwing errors. It will impact VPLS services. *Resolved In:* junos:20.4R3-S7 junos:20.4R3-S8
PR Number	**Synopsis**	**Category: ACX Interfaces IFD, IFL, vlans, and BRCM init**
1713699	The member interface will not be added to the AE bundle if the link-speed of the AE interface doesn't match that of the member Product-Group=junos	On Junos ACX5048 and ACX5096 platforms, if the link-speed is configured under the aggregated-ether-options hierarchy of the Aggregated Ethernet (AE) interface and the link-speed value does not match with the member link-speed, the member interface will not be added to the AE bundle. *Resolved In:* junos:20.4R3-S7 junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S4 junos:22.1R3-S2 junos:22.2R3-S1 junos:22.3R3 junos:22.4R2 junos:22.4R3 junos:23.1R1-S1 junos:23.2R1 junos:23.3R1
PR Number	**Synopsis**	**Category: "agentd" software daemon**
1665516	Na-grpcd process core observed in telemetry services Product-Group=junos	On all Junos and Junos OS Evolved platforms, due to race condition happening at the time of AFT streaming and simultaneous multiple attempts to subscribe and unsubscribe AFT sensors, followed by modifying firewall filter configurations, na-grpcd can core on rare occasions. This will cause a temporary outage of streaming telemetry services. The service will self-recover upon restart of the process. *Resolved In:* evo:20.4R3-S7-EVO evo:21.4R2-S1-EVO evo:21.4R3-EVO evo:21.4X1-EVO evo:22.1R3-EVO evo:22.3X50-EVO evo:22.3X80-D36-EVO evo:22.3X80-D37-EVO evo:22.4R2-EVO evo:23.1R1-EVO junos:20.3X75-D52 junos:21.4R3 junos:22.1R3 junos:22.4R2 junos:23.1R1
PR Number	**Synopsis**	**Category: PFE issue for flowd on australia SPU**
1727027	The datapath-debug packet-dump feature is not capturing the transit traffic packets Product-Group=junos	On SRX5000 platforms with IOC3 card (SRX5K-MPC3-100G10G and SRX5K-MPC3-40G10G) routing engine, datapath-debug packet-dump will stop capturing the transit traffic packets when datapath-debug packet filters with packet-dump are targeting the traffic on the interface which is configured with firewall filters. *Resolved In:* junos:20.4R3-S9 junos:21.2R3-S7 junos:22.2R3-S3 junos:23.2R2 junos:23.3R2 junos:23.4R1
PR Number	**Synopsis**	**Category: BBE OS Infrastructure library**
1732216	'max-db-size' configuration is optional in routers having DRAM greater than or equals to 32GB Product-Group=junos	On Junos MX platforms, to enable Enhanced Subscriber Management feature without 'max-db-size' configuration on router >=32GB DRAM(Dynamic Random Access Memory), router needs to be rebooted only once instead of rebooting twice.

		Resolved In: evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:20.2R3-S4-J9 junos:21.2R3-S5-J3 junos:21.2R3-S6 junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: Bi Directional Forwarding Detection (BFD)**
1725971	Multiple flaps of the interface will cause the BFD session to be down Product-Group=junos	On all Junos and Junos Evolved platforms, the IPv4 static route BFD (Bidirectional Forwarding Detection) session may stay down if the corresponding interface flaps multiple times. *Resolved In:* evo:21.4R3-S4-EVO evo:22.2R3-S1-EVO evo:22.3R3-EVO evo:22.4R2-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:21.2R3-S6 junos:21.4R3-S4 junos:22.1R3-S3 junos:22.2R3-S1 junos:22.3R3 junos:22.4R2 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
PR Number	**Synopsis**	**Category: Border Gateway Protocol**
1677935	Inter-domain forwarding connectivity will be broken between different lo0s in the option-C network causing problems for the MPLS transit-route Product-Group=junos	On all Junos and Evolved platforms, having BGP Labeled-Unicast (BGP-LU) and non-BGP route for same prefix/lo0 (loopback interface) and readvertising non-BGP active route for this prefix in BGP-LU, cause problems for MPLS transit-route. *Resolved In:* evo:21.4R3-EVO evo:22.1R3-EVO evo:22.2R2-EVO evo:22.2R3-EVO evo:22.3R1-EVO evo:22.3R2-EVO evo:22.4R1-EVO junos:21.2R3-S2-J1 junos:21.2R3-S3 junos:21.2R3-S4 junos:21.4R3 junos:22.1R3 junos:22.2R2 junos:22.2R3 junos:22.3R1 junos:22.3R2 junos:22.4R1
1690213	BMP will not send EOR message Product-Group=junos	On all Junos and Junos Evolved platforms, BMP(BGP Monitoring Protocol) will not send EOR(End of RIB) message for some releases. This will impact some data collections. *Resolved In:* 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
1742416	RPD scheduler slip is observed when the BGP session flaps and subsequent configuration changes for the same peer Product-Group=junos	On all Junos and Junos Evolved platforms, high CPU (RPD scheduler slips) leads to session timeouts/flaps for other protocols running in the system. *Resolved In:* evo:22.2R3-S3-EVO evo:22.2X100-EVO evo:22.3X50-EVO evo:22.3X80-D38-EVO evo:22.3X80-D39-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:20.3X75-D44 junos:20.3X75-D46 junos:20.3X75-D52 junos:21.2R3-S6 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S3 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
1754935	BGP multipath route is not correctly applied after changing the IGP metric Product-Group=junos	On all Junos and Junos Evolved platforms, multipath route is not correctly applied due to this Equal-cost multi-path (ECMP) will not be formed, when Border Gateway Protocol (BGP) multipath is configured and the Interior Gateway Protocol (IGP) metric of a network is modified and subsequently reverted. *Resolved In:* evo:23.2R2-EVO evo:23.3R2-EVO evo:23.4R1-EVO evo:24.1R1-EVO junos:23.2R2 junos:23.3R2 junos:23.4R1
1760885	The BGP LU labels can have next-hops pointing to each other in multi-homed PE setup Product-Group=junos	On all Junos and Junos Evolved platforms the routes received by two multi-homed PE (Provider Edge) routers in the 'inet-unicast' family are advertised in the BGP (Border Gateway Protocol) LU (Labeled Unicast) family to each other. This issue happens when there is no rib.inet3 configured under the address family labeled unicast which causes the routes from 'inet-unicast' and 'inet-labeled-unicast ' tables to get mixed. There will be a traffic impact when this issue is encountered.

		Resolved In: evo:22.1R3-S5-EVO evo:22.2R3-S3-EVO evo:23.2R2-EVO evo:23.3R2-EVO evo:23.4R1-EVO evo:24.1R1-EVO junos:21.2R3-S7 junos:22.2R3-J6 junos:23.2R2 junos:23.3R2 junos:23.4R1
PR Number	**Synopsis**	**Category: BBE Remote Access Server**
1687998	The authd process crashes during GRES recovery phase Product-Group=junos	On MX platforms, during recovery phase of Graceful Routing Engine Switchover (GRES), authd process crashes. *Resolved In:* evo:22.2R3-EVO evo:22.3R2-EVO evo:22.4R1-EVO evo:23.1R1-EVO junos:21.2R3-S3 junos:22.1R3 junos:22.2R2 junos:22.2R3 junos:22.3R1-S1 junos:22.3R2 junos:22.4R1 junos:23.1R1
PR Number	**Synopsis**	**Category: Express BT PFE L3 Features**
1611115	show pfe statistics traffic does not show host bound traffic Product-Group=junos	PFE level statistics for host bound traffic is coming zeros. *Resolved In:* evo:20.4R3-EVO evo:21.2R2-EVO evo:21.3R2-EVO evo:21.4R1-EVO junos:21.2R2 junos:21.3R2
PR Number	**Synopsis**	**Category: Virtual-chassis platform/chassisd infrastructure PRs for MX**
1713502	The firmware upgradation will fail for MPC7E line card in MX-VC scenario Product-Group=junos	On MX-VC platforms, the MPC7E firmware upgrade cannot be completed due to the TFTP (Trivial File Transfer Protocol) timeout error due to which the firmware image can't be put into FPC and the upgrade will not get succeed. *Resolved In:* evo:22.3R3-EVO evo:22.4R2-EVO evo:23.1R2-EVO evo:23.2R1-EVO junos:20.4R3-S7 junos:21.1R3-S5 junos:21.2R3-S5 junos:21.4R3-S4 junos:22.1R3-S2 junos:22.2R3-S1 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.1R2 junos:23.2R1
PR Number	**Synopsis**	**Category: Class of Service**
1760817	Change in the cosd behaviour due to the CoS interface specific wildcards Product-Group=junos	On all Junos platforms, applying the class-of-service (CoS) interface specific wildcards was leading to an inconsistent behaviour of the class-of-service daemon (cosd) at different times. *Resolved In:* evo:23.2R2-EVO evo:23.4R1-EVO evo:24.1R1-EVO junos:20.4R3-S9 junos:21.2R3-S7 junos:22.2R3-S3 junos:22.4R3 junos:23.2R2 junos:23.4R1
PR Number	**Synopsis**	**Category: CFM**
1682939	Maintenance-domain (MD) and Maintenance-association (MA) configuration display changed to ordered-by-system type Product-Group=junos	With this the maintenance-domain (MD) configuration and maintenance-association (MA configuration) under the connectivity-fault-management stanza will be ordered by the system and not as per the configuration order. *Resolved In:* evo:21.2R3-S6-EVO evo:21.4R3-S5-EVO evo:22.1R3-S4-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:21.2R3-S6 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:23.2R1 junos:23.3R1
PR Number	**Synopsis**	**Category: QFX Control Plane VXLAN**

1723968	Traffic loss is seen as Type 2 routes are not pushed even after withdrawing Type 5 routes Product-Group=junos	On all Junos and Junos Evolved platforms with the EVPN (Ethernet VPN) Type 2 and Type 5 Coexistence and when the host route changes from EVPN Type 5 route to non EVPN route in the rpd, traffic loss is observed as Type 2 routes are not getting pushed even after withdrawing Type 5 routes. *Resolved In:* junos:21.2R3-S6 junos:21.4R3-S4 junos:22.1R3-S3 junos:22.2R3-S1 junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
PR Number	**Synopsis**	**Category: 1G/10G LC Timing software**
1583496	Error message seen in clksyncd logs with SyncE/PTP configs "ESYNC-Error:ferrari_zl30362_reg_write: Error, EEC(0) not yet initialized" Product-Group=junos	Error message seen on MX10K8 chassis with SyncE/PTP configurations, This does not affect any functionality, The error seen here because the API called is specific to ferrari platform which needs to be vecterized. *Resolved In:* evo:22.3R2-EVO evo:22.4R2-EVO evo:23.1R1-EVO junos:21.2R3-S7 junos:22.2R3-S3 junos:22.3R2 junos:22.4R1 junos:22.4R2 junos:23.1R1
PR Number	**Synopsis**	**Category: Device Configuration Daemon**
1731190	The lt/vt/ut interfaces may not recover from the disable-pfe (admin down) state if the GRES switchover is done before restarting FPC Product-Group=junos	On all Junos Platforms when a PFE (Packet Forwarding Engine) gets disabled to a CM (Chassis Manager) error disable-pfe action or any other reason and a GRES (Graceful Routing Engine Switchover) happens, the lt/vt/ut (Logical Tunnel/Virtual Tunnel/Uplink Tunnel) interfaces will not recover after the FPC (Flexible PIC Concentrator) restart even though the error condition is recovered resulting in traffic loss. *Resolved In:* junos:20.4R3-J12 junos:20.4R3-S8 junos:21.2R3-S6 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: CoS support on DNX**
1704589	Traffic drops seen after making COS configuration change on ACX710 Product-Group=junos	On Junos ACX710 platforms, when CoS (Class-of-Service) scheduler changes are done for buffer usage and when traffic is flowing which involves bursty traffic, traffic drops are seen. *Resolved In:* junos:21.2R3-S6 junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: EVPN ELAN/E-TREE**
1689267	FPC crashes and goes into down or unknown state in a scaled EVPN setup Product-Group=junos	On Junos ACX5448 and ACX710 platforms with scaled EVPN (Ethernet Virtual Private Network) setup, a 'restart routing' can trigger the PFE (Packet Forwarding Engine) crash and the FPC (Flexible PIC Concentrator) will get stuck either in down or unknown state resulting in a total traffic impact. *Resolved In:* junos:21.2R3-S6 junos:21.4R3-S3 junos:22.1R3-S2 junos:22.1R3-S4 junos:22.2R3 junos:22.3R3 junos:22.3R3-S1 junos:22.4R2 junos:22.4R3 junos:23.1R1
PR Number	**Synopsis**	**Category: VPWS, L2 CKT, EVPN-VPWS**
1683900	The traffic drop is observed in the l2circuit scenario with control-word configuration	On Junos ACX5448/ACX710 platforms in the layer2 circuit (l2circuit) scenario, if the control-word configuration is enabled/disabled, the complete traffic drop is observed for the affected l2circuit.

	Product-Group=junos	*Resolved In:* junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S1 junos:22.1R3 junos:22.2R3 junos:22.3R2 junos:22.4R1 junos:23.1R1
PR Number	**Synopsis**	**Category: DNX Multicast**
1643598	In EVPN multihoming, BUM traffic from the CE device will be flooded back to the CE device Product-Group=junos	On all Junos platforms, EthernetVPN Multi-Protocol Label Switching/Ethernet-Tree (EVPN-MPLS/EVPN-E-Tree) Broadcast Unknown-unicast and Multicast (BUM) traffic received on Non-Designated Forwarder (Non-DF) will be forwarded back to Customer Device (CE) via Designated Forwarder (DF) when CE-DF link flap. *Resolved In:* junos:21.2R3-S7 junos:21.3R3 junos:21.4R3 junos:22.1R2 junos:22.2R1 junos:22.2R2 junos:22.3R1
PR Number	**Synopsis**	**Category: EVPN Layer-2 Forwarding**
1702016	ARP/ND doesn't resolve when extended-vlan-list is configured for the specific VLAN Product-Group=junos	On all Junos & Junos Evolved platforms, ARP(Address resolution protocol)/ND(Neighbour discovery) doesn't resolve when extended-vlan-list is configured for the specific VLAN(virtual local area network). *Resolved In:* evo:22.2R3-EVO evo:22.3R3-EVO evo:22.4R2-EVO evo:23.1R1-EVO evo:23.2R1-EVO junos:20.4R3-S7 junos:21.1R3-S5 junos:21.2R3-S4 junos:21.3R3-S4 junos:21.4R3-S3 junos:22.1R3-S1 junos:22.2R3 junos:22.3R2 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.2R1
1718165	ARP learning issues are observed post-execution of the CLI command 'clear bridge mac-table' or 'clear ethernet-switching table' in the EVPN-MPLS over IRB environment Product-Group=junos	On all Junos and Junos Evolved platforms, L3 (Layer 3) traffic will be impacted when ARP (Address Resolution Protocol) entries get deleted for the MAC (Media Access Control) address having a bad state post execution of the CLI 'clear bridge mac-table' or 'clear ethernet-switching table' command in the EVPN-MPLS (Ethernet VPN - Multiprotocol Label Switching) over IRB (Integrated routing and bridging) environment. *Resolved In:* evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:21.2R3-S7 junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: EX4100 PFE**
1681478	Multicast traffic loss is seen with 'igmp-snooping' running on EX4100 Product-Group=junos	On Junos EX4100 platforms, multicast traffic drop happens if IGMP (Internet Group Management Protocol) snooping is configured without an IRB (Integrated Routing and Bridging) interface association. *Resolved In:* junos:22.1R3-S4 junos:22.2R2 junos:22.2R3 junos:22.3R1 junos:22.3R1-S1 junos:22.3R2 junos:22.4R1 junos:23.1R1
PR Number	**Synopsis**	**Category: EX4100 RE, Platform Infra, Drivers**
1747277	[EX/QFX] Under rare situations, 10GBASE-T SFP might be unable to make the peer end deivce linkdown. Product-Group=junos	Under rare situations, EX/QFX5K 10GBASE-T SFP might be unable to make the peer end deivce linkdown. This is because Junos did not disable Tx on 10G BASE-T PHY under rare situations. *Resolved In:* junos:22.4R3 junos:23.3R2 junos:23.4R1
PR Number	**Synopsis**	**Category: EX4400 PFE software**

1698833	The DHCP offer packet failed to send back to the client leaf from the server leaf Product-Group=junos	On EX4100, EX4400 and QFX5k platforms, when inter-vrf DHCP relay is configured, the server leaf fails to send the DHCP offer response packet to the client leaf. Due to this DHCP client will not be able to bind. *Resolved In:* junos:21.4R3-S4 junos:22.1R3-S2 junos:22.2R3-S1 junos:22.3R2-S1 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.2R1
1738384	The 'input-vlan-map push' operation will not work on double-tagged frames Product-Group=junos	On EX4400 platforms, when 'input-vlan-map push' is configured to push an outer VLAN (Virtual Local Area Network) tag on to a double-tagged frame, the egressing frame will be tagged incorrectly. Instead of a push operation, the outer VLAN tag of the ingressing double-tagged frame will be swapped and sent out. This results in unexpected behaviour or traffic loss as the Ethernet frames will not have the expected VLAN tag information. *Resolved In:* junos:22.1R3-S4 junos:22.2R3-S1 junos:22.3R2-S2 junos:22.3R3-S1 junos:22.4R2-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
1747878	Packet drop will be observed due to ARP resolution failure in EVPN-VXLAN scenario Product-Group=junos	On Junos Evolved ACX/SRX/QFX/EX (BROADCOM based) platforms, ARP (Address Resolution Protocol) resolution is unsuccessful and packet drop will be seen, when interface mode - access is configured in EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) ERB (Edge Routed Bridging) scenario. *Resolved In:* junos:21.2R3-S7 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R2-S2 junos:22.4R3 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: EX4400 platform**
1720074	Port will be down when "no-auto-negotiation" is configured on EX4400-48F platform Product-Group=junos	On EX4400-48F platform with Small Form Factor Pluggable 100Base-FX Fast Ethernet Optics, when "no-auto-negotiation" is configured on the interface this results in the interface not coming back online even after deleting "no-auto-negotiation" in interface. *Resolved In:* junos:21.2R3-S6 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R2-S2 junos:22.3R3-S1 junos:22.4R2-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
1734435	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. *Resolved In:* 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
1741724	On EX4400 with pre existing configuration of 1g for the uplink interfaces, it might not come up after 4x10G module insertion event Product-Group=junos	EX4400: With pre existing configuration of 1g for the uplink interfaces, the 1G uplink ports might not come up on 4x10G module insertion event. *Resolved In:* junos:22.4R3 junos:23.2R2 junos:23.4R1
1753576	Runt frames generate excessive traffic statistics on EX4100/EX4400 platforms Product-Group=junosvae	On EX4100/EX4400 platforms with Multi-rate gigabit ethernet (MGE) ports , incorrect register is read for the runt counter and the calculation logic generates a big value. As these bytes are part of input octets, it displays incorrect value. *Resolved In:* junos:21.3R3-S5 junos:21.4R3-S5 junos:22.2R3-S2 junos:22.3R2-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.3R2

		junos:23.4R1
PR Number	**Synopsis**	**Category: PFE EVPN / VxLAN related issues on EX platforms**
1693967	DHCP binding fails after dot1x authentication in EVPN-VXLAN network Product-Group=junos	On Junos EX4100, EX4400 and EX4650 platforms, in the VXLAN (Virtual Extensible LAN) network, DHCP (Dynamic Host Configuration Protocol), ARP (Address Resolution Protocol) and PING services will get impacted as the DHCP binding fails due to the DHCP offer packet being tagged while egressing out of the DHCP relay agent when Dot1x is authenticated on a port. *Resolved In:* junos:21.4R3-S4 junos:22.1R3-S2 junos:22.2R3-S1 junos:22.3R2-S1 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.1R2 junos:23.2R1
PR Number	**Synopsis**	**Category: Express pfe Mclag**
1610173	Continuous L3 traffic drop might be observed with MC-LAG configuration on QFX10K platforms Product-Group=junos	On QFX10K platforms with MC-LAG configured, When trying to add or remove the MC-LAG configuration continuous L3 traffic drop might be observed which might not be recovered. *Resolved In:* junos:20.4R3-S1 junos:21.1R2-S2 junos:21.1R3 junos:21.2R1-S2 junos:21.2R2 junos:21.2R2-S1 junos:21.2R3 junos:21.3R1-S1 junos:21.3R2 junos:21.4R1 junos:22.1R1
PR Number	**Synopsis**	**Category: FIPS related issues**
1623128	The device will be unavailable while performing FIPS 140-2/FIPS 140-3 level 2 internal test on FreeBSD 12 based Junos platforms Product-Group=junos	When Federal Information Processing Standards (FIPS) 140-2/140-3 defines security level 2 is enabled on the FreeBSD 12 based Junos platforms, the series of known answer test (KAT) self-tests will be performed automatically and stuck in kernel_kats test due to unsupported FIPS features, then the device will be unreachable or will be rebooted again and again, there is no impact to the customer since some FIPS 140-2/140-3 level2 features do not apply to FreeBSD 12 officially. *Resolved In:* evo:21.4R2-EVO evo:22.1R1-EVO evo:22.2R1-EVO junos:21.4R2 junos:22.1R1 junos:22.2R1
PR Number	**Synopsis**	**Category: ACX500/1000/2000/4000 timing software**
1755852	[TWM Clocking Solution] - PTP packets are not processed over GE interfaces of ACX2200 with latest respin image 21.2R3-S6.10 Product-Group=junos	Due to software issue with initialization sequence, the PTP encapsulation does not get applied with PTP configuration on ge interfaces. Because of this, PTP feature is impacted on ge interfaces. *Resolved In:* junos:21.2R3-S7
PR Number	**Synopsis**	**Category: SRX4100/SRX4200 platform software**
1630981	IPSec VPN traffic might get dropped on SRX4100/SRX4200 Product-Group=junosvae	All VPN traffic may internally drop during encryption / decryption processing in HW engine requiring PFE plane reset. *Resolved In:* junos:20.4R3-S7 junos:21.4R3-S3 junos:22.4R3 junos:23.2R1 junos:23.3R1
PR	**Synopsis**	**Category: idp flow creation, deletion,notification, session mgr intfce**

Number		
1705491	Network outage caused during change in IDP policy Product-Group=junos	Junos SRX platforms experience traffic outage during change in IDP (Intrusion Detection and Prevention) policy. *Resolved In:* junos:21.1R3-S5 junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S3 junos:21.4R3-S4 junos:22.1R3-S1 junos:22.1R3-S2 junos:22.2R3 junos:22.2R3-S1 junos:22.3R2 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.2R1
PR Number	**Synopsis**	**Category: Signature Database**
1741887	Multiple network issues are seen after the upgrade with lower IDP packet-log total-memory percentage Product-Group=junos	On Junos SRX platforms, before the upgrade, if the IDP 'packet-log total-memory percentage/packet-log max-sessions' is configured lower than the default value of 10% then while upgrading, the boot time commit will fail and the device will go to an amnesiac state causing multiple issues. *Resolved In:* junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: Kernel software for AE/AS/Container**
1747289	VRRP traffic will drop when the member link from the AE bundle is deleted, even if there are active members in the AE bundle Product-Group=junos	On Junos using afeb/tfeb way of communication to PFE that is MX80/MX104 platforms with Virtual Router Redundancy Protocol (VRRP) configured, deleting a member link from the Aggregated Ethernet (AE) bundle removes the VRRP filter entry in the Packet Forwarding Engine (PFE) which causes VRRP traffic to get dropped even though other active member links in the AE bundle exists. *Resolved In:* junos:20.4R3-S9
PR Number	**Synopsis**	**Category: ISIS routing protocol**
1719033	The rpd process crashes when TI-LFA is enabled Product-Group=junos	On all Junos and Junos Evolved platforms, the rpd is seen to crash when TI-LFA (Topology-Independent Loop-Free Alternate) is enabled and there are ECMP (Equal-Cost Multipath) routes present. *Resolved In:* evo:22.3R3-EVO evo:22.3X50-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:21.2R3-S6 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R2-S2 junos:22.3R3 junos:22.4R2 junos:22.4R3 junos:23.1R1-S1 junos:23.1R2 junos:23.2R1 junos:23.3R1
1725686	Unnecessary SPF calculation is causing high CPU utilization Product-Group=junos	On all Junos and Junos Evolved platforms, very frequent SPF (Shortest Path First) calculation, being caused by leaking multiple prefixes across the IS-IS areas, is causing high CPU utilization. *Resolved In:* evo:21.2R3-S6-EVO evo:21.4R3-S4-EVO evo:22.1R3-S4-EVO evo:22.2R3-S2-EVO evo:22.4R2-S1-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:20.4R3-S7-J2 junos:20.4R3-S8 junos:21.2R3-S6 junos:21.4R3-S4-J3 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.2R2 junos:23.3R1
1753003	The rpd crashes on all Junos and Junos Evolved platforms with IS-IS, segment routing and flex algo configured Product-Group=junos	On all Junos and Junos Evolved platforms, with IS-IS, segment routing and flex algorithm enabled, when the route from ribgroup is deleted due to interface flap, it leads to crash of the infra module as route entry table does not match with the rtbit table (which is passed from IS-IS). *Resolved In:* evo:21.2R3-S7-EVO evo:22.2R3-S3-EVO evo:22.3R3-S2-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.3R2-EVO evo:23.4R1-

		EVO junos:21.2R3-J12 junos:21.2R3-S5-J16 junos:21.2R3-S7 junos:22.2R3-S3 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.3R2 junos:23.4R1
PR Number	**Synopsis**	**Category: Flow Module**
1705996	A flowd process crash is seen on SRX4100/4200/4600, vSRX, and SRX5K with SPC3 card when a route is changed frequently Product-Group=junos	In a race condition, when PMI (power-mode-ipsec) is enabled and routes are changing frequently (3~5sec) on SRX4100/4200/4600, vSRX, and SRX5K with SPC3 card, a flowd process crash will be seen. *Resolved In:* junos:20.4R3-S6 junos:21.2R3-S4 junos:21.3R3-S4 junos:21.4R3-S3 junos:21.4R3-S5 junos:22.1R3-S1 junos:22.1R3-S3 junos:22.2R3 junos:22.2R3-S2 junos:22.3R2 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.2R1
1755181	SRX5k or SRX4600 is forwarding the traffic with OLD MAC address, even though the ARP table is pointing to a new MAC address. Product-Group=junos	On SRX5000 series and SRX4600, for flow sessions which are using Express Path (a.k.a. Service Offload), the next-hop MAC address will not be updated for existing sessions, when the ARP table entry for the next-hop IP address changes. This may for example occur on VRRP failovers of directly connected routers if they do not use a virtual MAC address or server load balancers failing over the VIP to a new device with a different MAC address. Note that from Junos 21.2 onwards, Express Path is enabled by default. *Resolved In:*
1761891	Multicast packets of specific size between 663 - 676 bytes getting dropped Product-Group=junos	On SRX platforms, due to the incorrect size of memory allocated in mbuf (Memory Buffer) multicast packets of specific sizes between 663 - 676 bytes get dropped resulting in multicast traffic impact. *Resolved In:* junos:21.2R3-S7 junos:23.2R2 junos:23.4R1
PR Number	**Synopsis**	**Category: User Firewall related issues**
1755593	Users authenticated via captive portal experience a noticeable delay of atleast 2-5 mins Product-Group=junos	On all SRX platforms, the user-firewall configuration in policy with push-to-identity enabled may cause a delay in web-authenticating the users. *Resolved In:* junos:21.2R3-S6-J3 junos:21.2R3-S7 junos:22.1R3-S4 junos:22.4R3 junos:23.2R2 junos:23.3R2 junos:23.4R1
PR Number	**Synopsis**	**Category: IPSEC/IKE VPN**
1696102	IPsec VPNs will disconnect after ISSU Product-Group=junos	On SRX platforms except SRX5K, & vSRX2.0/vSRX3.0, traffic will not pass over IPsec (Internet Protocol Security) VPN tunnels after ISSU (In-service software upgrade). *Resolved In:* junos:21.2R3-S5 junos:21.4R3-S3 junos:22.1R3-S2 junos:22.2R3 junos:22.3R3 junos:22.4R2 junos:23.1R2 junos:23.2R1
PR Number	**Synopsis**	**Category: Security platform jweb support**
1698386	Junos OS: J-Web: Multiple Vulnerabilities in PHP software Product-Group=junos	PHP software included with Junos OS J-Web has been updated from 7.4.30 to 8.2.0 to resolve multiple vulnerabilities. Please refer to https://supportportal.juniper.net/JSA71653 for more information. *Resolved In:* evo:23.2R1-EVO evo:23.3R1-EVO junos:23.2R1 junos:23.2R2 junos:23.3R1
1748078	Cannot add custom defined	In the J-Web UI for SRX Series Firewall, when you configure the source zone for

	security address-book under Security Policies & Objects > Security Policies > Create > Source Zone > Select Sources. Product-Group=junos	addresses in the security policy rule, the customized address-book entries are not displayed. J-Web displays only any-ipv4 and any-ipv6. *Resolved In:* junos:21.2R3-S6 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: Layer2 forwarding on EX/NTF/PTX/QFX**
1724489	Help string "Display information for a specified VLAN" is changed to "Display information for a specified bridge domain" Product-Group=junos	On Junos MX platforms, the help string for CLI command "show mac-vrf forwarding flood ?" vlan-name is changed from "Display information for a specified VLAN" to "Display information for a specified bridge domain" *Resolved In:* evo:23.2R2-EVO evo:23.3R2-EVO evo:23.4R1-EVO evo:24.1R1-EVO junos:20.4R3-S9 junos:21.2R3-S7 junos:22.2R3-S3 junos:22.4R3 junos:23.2R2 junos:23.3R2 junos:23.4R1
1727954	On all Junos and Junos Evolved platforms the l2ald process memory usage is seen to increase over time Product-Group=junos	On all Junos and Junos Evolved platforms service impact is seen due to a consistent increase in l2ald (Layer 2 Address Learning Daemon) memory usage. *Resolved In:* evo:21.2R3-S6-EVO evo:21.4R3-S4-EVO evo:22.1R3-S4-EVO evo:22.2R3-S2-EVO evo:22.3R3-S1-EVO evo:22.3X50-EVO evo:22.4R2-S2-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:21.2R3-S6 junos:21.4R3-S4 junos:22.1R3-S3 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R2-S2 junos:22.4R3 junos:22.4R3-S1 junos:23.1R2 junos:23.2R1 junos:23.2R2 junos:23.3R1 junos:23.4R1
1743282	The l2ald crashes when there is recursive deletion of IFBD or when BGP neighborship is cleared in EVPN-VXLAN multi-homed configuration Product-Group=junos	On all Junos and Junos OS Evolved platforms, in a rare scenario, due to timing issue, the l2ald (Layer 2 Address Learning Daemon) crashes and traffic is being blackholed due to recursive deletion of IFBD (Interface Family Bridge Domain) or when BGP (Border Gateway Protocol) neighborship is cleared when EVPN (Ethernet Virtual Private Network) - VXLAN (Virtual Extensible Local Area Network) with multi-homed is configured. *Resolved In:* evo:20.4R3-S9-EVO evo:21.2R3-S6-EVO evo:21.4R3-S5-EVO evo:22.1R3-S4-EVO evo:22.2R3-S2-EVO evo:22.3R3-S1-EVO evo:22.4R2-S2-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-S1-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:20.4R3-S9 junos:21.2R3-S6 junos:21.4R3-S4 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R2-S2 junos:22.4R3 junos:23.1R2 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: SW PRs for MPC10E Fabric**
1676777	Traffic drop can be seen on MX platforms with MPC10E-10C line card Product-Group=junos	On MX platforms with MPC10E-10C line card, with line rate traffic, continuous traffic drop can be seen when fabric mode is changed from increased bandwidth to redundant. *Resolved In:* evo:22.1R3-EVO evo:22.2R2-EVO evo:22.2R3-EVO evo:22.3R2-EVO evo:22.4R1-EVO junos:20.3X75-D46 junos:20.4R3-S8 junos:21.2R3-S3 junos:21.2R3-S6 junos:21.3R3-S3 junos:21.4R3-S1 junos:21.4R3-S4 junos:22.1R3 junos:22.1R3-S3 junos:22.2R2 junos:22.2R3 junos:22.3R2 junos:22.4R1
PR Number	**Synopsis**	**Category: SW PRs for MPC10E Interfaces**
1688972	PFE wedge will be seen due to fast link flaps Product-Group=junos	When the 10/40/100G links of the same PFE (Packet Forwarding Engine) on MPC10E/MPC11E/LC2301/MX10K-LC9600 line cards flap continuously, the whole PFE can wedge and all the links in that PFE will be affected.

		Resolved In: evo:22.3R3-EVO evo:22.4R2-EVO evo:23.1R1-EVO evo:23.2R1-EVO junos:20.3X75-D46 junos:20.4R3-S7 junos:21.1R3-S5 junos:21.2R3-S2-J8 junos:21.2R3-S3-J10 junos:21.2R3-S4 junos:21.4R3-S3 junos:22.2R3 junos:22.3R2 junos:22.3R3 junos:22.4R2 junos:22.4R3 junos:23.1R1 junos:23.2R1
PR Number	**Synopsis**	**Category: Multiprotocol Label Switching**
1738774	Traffic blackhole due to an additional label when CCNH is toggled Product-Group=junos	On all Junos and Junos Evolved platforms, with scaled Border Gateway Protocol (BGP) routes, when Chained Composite Next Hops (CCNH) is toggled, a few next-hops end up creating additional labels causing a traffic blackhole. *Resolved In:* evo:21.4R3-S5-EVO evo:22.3X50-EVO evo:22.3X80-D36-EVO evo:22.3X80-D38-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:21.2R3-S4-J27 junos:21.2R3-S6 junos:21.4R3-S5 junos:22.4R2-S2 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: For multicast snooping on MX**
1699784	The mcscnoopd process will be stuck in resync state after snooping configuration is deleted and added again immediately Product-Group=junos	On all Junos platforms, when the multicast snooping configuration is deleted and added again immediately, the mcscnoopd (multicast-snooping process daemon) process will be stuck in the resync state, impacting the multicast traffic. *Resolved In:* evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:21.4R3-S4 junos:22.2R3-S2 junos:22.3R2-S2 junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: MX l2ng access security**
1627611	DHCP clients might not go to BOUND state when the AE bundle is enabled between DHCP server and snooping device Product-Group=junos	On Junos platforms with MPC10E line cards, when AE under the IRB interface is enabled between the snooping device and the DHCP server, the DHCP bindings can be seen in snooping device and DHCP server, but the DHCP client might not go to BOUND state, it might be stuck at discovering/requesting state. *Resolved In:* evo:22.1R1-EVO junos:21.2R3-S6 junos:21.4R2 junos:22.1R1
PR Number	**Synopsis**	**Category: MX Timing software**
1652275	PTP Playback Engine reset error is reported sporadically with PTP FPGA Firmware version A4 7 Product-Group=junos	On Junos MX platforms, the PTP Playback Engine reset error is reported sporadically with PTP FPGA Firmware version A4 7. It has No functionality impact. *Resolved In:* evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:20.4R3-S8 junos:21.2R3-S6 junos:22.2R3-S2 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
1664569	Switch Fabric Board information for supporting PTP on MX10k8 with MX10K-LC2101 LC(s) Product-Group=junos	MX10k8 with MX10K-LC2101 Linecard(s) supports *PTP* only with JNP10008-SF Switch Fabric Board(s), *PTP* currently doesn't work with JNP10008-SF2 Switch Fabric Board(s). *Resolved In:* evo:22.2R3-EVO evo:22.3R2-EVO evo:22.4R2-EVO evo:23.1R1-EVO junos:20.4R3-S8 junos:21.2R3-S6 junos:22.2R3 junos:22.3R2 junos:22.4R1 junos:22.4R2 junos:23.1R1
1696957	In the rare scenario, huge PTP	On MX240, MX480, MX960, MX2010, and MX2020 platforms, the remote PTP

	Time errors are introduced and propagated to the downstream devices after the chassis reboot Product-Group=junos	(Precision Time Protocol) clock will recover the PTP clock with Time errors after a chassis reboot on the device running as Boundary Clock. *Resolved In:* evo:22.3R3-EVO evo:22.4R2-EVO evo:23.1R1-EVO evo:23.2R1-EVO junos:20.4R3-S6 junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S3 junos:22.2R3 junos:22.3R2 junos:22.3R3 junos:22.4R1-S1 junos:22.4R2 junos:23.1R1 junos:23.2R1
1704633	Interface flaps are seen after PTP GM changes to a different FPC slot Product-Group=junos	On MX platforms, when PTP (Precision Time Protocol) is configured, the interfaces will flap after the PTP GM (Grand Master) is changed to a different FPC (Flexible PIC Concentrators) slot. The flaps can last for several seconds. Chassis-SyncE clock is also influenced by PTP phase change. *Resolved In:* evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:20.4R3-S8 junos:21.2R3-S6 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
1738458	PTP time sync issues after release upgrade or rebooting the device Product-Group=junos	On all MX platforms with 20x1GE MICs (Modular Interface Card), PTP (Precision Time Protocol) downstream client cannot receive an accurate clock from the router after an upgrade or FPC restart which impacts the PTP functionality. *Resolved In:* junos:21.2R3-S6 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
1750316	SyncE stuck in holdover upon PTP slot switchover without change in PTP phase align state Product-Group=junos	SyncE stuck in holdover upon PTP slot switchover without change in PTP phase align state. *Resolved In:* junos:20.4R3-S9 junos:21.2R3-S6 junos:22.1R3-S4 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.3R2 junos:23.4R1
1750885	MPC10E: Support of G.8275.1 PTP Hybrid mode with speed 25G and 400G Product-Group=junos	In 21.2R3S6 release, MPC10E line-card does not support of G.8275.1 PTP Hybrid mode with speed 25G and 400G *Resolved In:* evo:23.4R1-EVO evo:24.1R1-EVO junos:21.2R3-S7 junos:23.2R2 junos:23.4R1
PR Number	**Synopsis**	**Category: MX104 Software - Chassis Daemon**
1747532	The PFE crash will be observed when configuring the 'per-unit-scheduler' on the MACSEC MIC interface Product-Group=junos	On MX104 platform with MACSEC MIC, the 'per-unit-scheduler' configuration on the MACSEC MIC interface results in the PFE crash leading to traffic impact. *Resolved In:* junos:20.4R3-S9 junos:21.2R3-S7
PR Number	**Synopsis**	**Category: Microkernel for neo mpc**
1670137	Multibit ECC error causes the whole MX Series router chassis to go down Product-Group=junos	Faulty Flexible PIC Concentrator (FPC) on the MX Series router chassis exhibiting multibit error checking and correction (ECC) error (L2 cache error) will trigger the whole chassis to go down. The whole chassis goes down until the faulty FPC is removed from the chassis. *Resolved In:* junos:20.3X75-D36 junos:20.4R3-S4-J11 junos:20.4R3-S8 junos:21.2R3-S4 junos:21.4R3-S3 junos:22.2R3 junos:22.3R2 junos:22.4R1 junos:22.4R2
PR Number	**Synopsis**	**Category: OS IPv4/ARP/ICMPv4**
1763706	Routing Protocol session down	On certain Junos MX platforms, the IS-IS (Intermediate System to Intermediate

	with native VLAN configuration on MX platforms Product-Group=junos	System) sessions will not come up/keep flapping when the native VLAN (Virtual Local Area Network) is configured on the associated l3 interface. There will be traffic loss due to the routing protocols being down and the workaround for the issue is to remove the native VLAN configuration. *Resolved In:* junos:21.2R3-S7 junos:22.2R3-S3 junos:22.4R2-S2 junos:22.4R3 junos:23.2R2 junos:23.3R2 junos:23.4R1
PR Number	**Synopsis**	**Category: FreeBSD Kernel Infrastructure**
1568757	The image validation is not supported during upgrading from Pre 21.2 to 21.2 and onward Product-Group=junos	When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. https://kb.juniper.net/TSB18251 *Resolved In:*
1681783	On Ex4400 upgrade failure happens when upgrading through a USB drive. Product-Group=junos	On EX4400 upgrade failure happens when upgrading through a USB drive. *Resolved In:* junos:19.1R3-S10 junos:19.2R3-S7 junos:19.4R3-S10 junos:20.3R3-S6 junos:20.3X75-D43 junos:20.3X75-D46 junos:20.3X75-D52 junos:20.4R3-S5 junos:21.2R3-S3 junos:21.2R3-S4 junos:21.3R3-S2 junos:21.3R3-S3 junos:21.4R3-S1 junos:21.4R3-S4 junos:22.1R2-S1 junos:22.1R2-S2 junos:22.1R3 junos:22.2R1-S2 junos:22.2R2 junos:22.2R2-S1 junos:22.2R3 junos:22.3R1-S1 junos:22.3R2 junos:22.4R1
PR Number	**Synopsis**	**Category: "ifstate" infrastructure**
1735685	Control plane flap, data drop, unexpected behavior of PFE or device is observed when file storage is impacted in a continuous ksyncd process crash scenario Product-Group=junos	On all Junos platforms configured with GRES (Graceful Routing Engine Switchover), file storage in the system will get affected when the ksyncd process crashes continuously and result in control plane flap, data drop or unexpected behavior of PFE (Packet Forwarding Engine) or device. *Resolved In:* junos:21.2R3-S7 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R2-S2 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: PFE Peer Infra**
1747077	Error message: 'Minor potential slow peers are: X' seen on Junos based platforms Product-Group=junos	On all Junos platforms with dual RE, error message: 'Minor potential slow peers are: X' will be seen. Due to some reason the PFE/PIC will be slow and services will face latency issue. the peerbuf list gets full, peer proxy could not enqueue further IPCs (ifstate chain/peer update to backup gets stalled) causing pfe/pics to be a slow consumer, this impacts service on the device. *Resolved In:*
PR Number	**Synopsis**	**Category: Kernel Tunnel Interface Infrastructure**
1712352	Master and Backup RE synchronization issue will be seen if chassisd is restarted on Master RE Product-Group=junos	On all Junos platforms with GRES (Graceful Routing Engine Switchover) and NSR (Non Stop Routing) enabled, Master and Backup RE (Routing-Engine) synchronization issues will be seen when chassisd (Chassis process) is restarted on Master RE. The ksyncd (Kernel Synchronization) process crash will be observed on the backup RE. If failover happens post this event, traffic would be impacted. This is a rare issue. *Resolved In:* junos:22.4R2-S2 junos:22.4R3 junos:23.2R1 junos:23.3R1

PR Number	Synopsis	Category: Express Chip L3 software
1743978	GRE over IPv6 will not work resulting in traffic impact post-upgrading the device Product-Group=junos	On QFX10002-60C platform, GRE (Generic routing encapsulation) for IPv6 will not work resulting in traffic impact due to software issues post-upgrading the device from lower than 21.3R1 release. *Resolved In:* junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1 junos:23.4R1
1761579	The FPC will crash on Junos PTX platforms in a rare timing issue Product-Group=junos	On Junos PTX platforms with with FPC3, JNP10K-LC1101, JNP10K-LC1102, JNP10K-LC1104, JNP10K-LC1105 and PTX10000, during a rare race condition in hostbound packet handler thread, the FPC (Flexible PIC Concentrator) might crash leading to all the interfaces going down. The exact trigger for this issue is unknown. *Resolved In:* junos:20.4R3-S9 junos:21.2R3-S7 junos:22.2R3-S3 junos:22.4R3 junos:23.2R2 junos:23.3R2 junos:23.4R1
PR Number	**Synopsis**	**Category: Path computation client daemon**
1690668	The rpd process will crash when externally provisioned LSPs are reconfigured by the controller or the global MPLS configuration is changed Product-Group=junos	On all Junos OS and Junos OS Evolved platforms, if LSPs are reconfigured by the controller or the global Multi Protocol Label Switching (MPLS) configuration is changed it leads to an rpd crash and results in traffic loss. *Resolved In:* evo:21.2R3-S4-EVO evo:21.3R3-S3-EVO evo:21.4R3-S2-EVO evo:22.1R3-EVO evo:22.2R2-EVO evo:22.2R3-EVO evo:22.3R2-EVO evo:22.4R1-EVO evo:23.1R1-EVO junos:21.2R3-S4 junos:21.3R3-S3 junos:21.4R3-S2 junos:22.1R3 junos:22.2R2 junos:22.2R3 junos:22.3R2 junos:22.4R1 junos:23.1R1
PR Number	**Synopsis**	**Category: vMX Data Plane Issues**
1669261	vMX crashes due to MBUF leaks Product-Group=junos	vMX platforms (MX150) will crash as a result of the MBUF (Memory Buffer) leak. *Resolved In:* junos:20.3X75-D43 junos:20.3X75-D46 junos:20.4R3-S5 junos:21.4R3 junos:22.1R3 junos:22.3R1 junos:22.3R2 junos:22.3R3 junos:22.4R2 junos:22.4R3 junos:23.1R1
PR Number	**Synopsis**	**Category: Protocol Independant Multicast**
1675212	High CPU utilization is seen when chassisd is down during dynamic IFL creation Product-Group=junos	On all Junos platforms, in a very rare cases, while creating the specific dynamic IFls (PE-PIM (Protocol Independent Multicast) Encapsulation or PD-PIM Decapsulation), if the chassisd is down, the stuck entries in the Kernel Routing table (KRT) queue results in a high CPU utilization. The high CPU might hamper the rpd process functionality in rare cases and also device responsiveness will be slow. *Resolved In:* evo:21.2R3-S7-EVO evo:22.2R3-S1-EVO evo:22.3R1-S2-EVO evo:22.3R2-EVO evo:22.4R1-EVO evo:23.1R1-EVO junos:21.2R3-S7 junos:21.4R3-S2 junos:22.2R3-S1 junos:22.3R1-S2 junos:22.3R2 junos:22.4R1 junos:23.1R1
PR Number	**Synopsis**	**Category: Issues related to PKI daemon**
1739342	Memory leak in PKID Product-Group=junos	PKID process shows memory usage increase over time after a larger number of certificate verifications. The issue can be recovered by the CLI command "restart pki-service".

		Resolved In: evo:21.2R3-S6-EVO evo:21.4R3-S5-EVO evo:22.1R3-S4-EVO evo:22.2R3-S2-EVO evo:22.3R3-S1-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:21.2R3-S6 junos:21.4R3-S3-J5 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R2-S2 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: Periodic Packet Management Daemon**
1739860	The IPv6 link local based BFD session over an AE interface will be stuck in Init state Product-Group=junos	On all MX platforms, when chassis network-services is set in IP mode, the IPv6 Link Local based BFD session over an AE interface will be stuck in init due to the next-hop misprogramming in the PFE. *Resolved In:* evo:22.3X80-D38-EVO evo:22.3X80-D39-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:21.2R3-S6 junos:21.2X33-J7 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: QFX platform fabric mgmt for Express ASIC chip**
1734735	Packet drop is observed due to SIB ASIC issue on fabric Product-Group=junos	On all inserted FPCs of Junos based QFX10K8/QFX10K16 platforms,due to SIB (Switch Interface Board) ASIC (Application-Specific Integrated Circuit) issue on fabric, packets are getting dropped and major errors "PECHIP_CMERROR_EPW_MISC_INT_EVENTS_CRC_ERR (0x2101aa)" are reported. These errors are not auto-cleared on a couple of FPCs. *Resolved In:* junos:20.4R3-S8 junos:21.2R3-S6 junos:21.4R3-S5 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: QFX PFE Class of Services**
1726124	The class of service subsystem crashed after the device is restarted or the switchover is performed Product-Group=junos	On Junos QFX5100 and QFX5110 platforms in virtual chassis, the cosd crash is observed when the GRES (Graceful Routing Engine Switchover) is performed or the device is restarted, due to which the Class of Service (CoS) functionality will not work. It is a rare issue. *Resolved In:* junos:20.4R3-S8 junos:21.2R3-S6 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: QFX EVPN / VxLAN**
1625285	Traffic loss might be observed after configuring VXLAN over IRB interface Product-Group=junos	On QFX5100/QFX5110/QFX5200/QFX5210/EX4300-48MP/EX4600/EX4650-48Y platforms, with IRB interface as underlay for VXLAN, data plane VXLAN traffic loss might be observed. *Resolved In:* junos:21.2R2-S1 junos:21.2R3 junos:21.3R2 junos:21.4R1 junos:21.4R2 junos:22.1R1
1688323	Traffic loss is observed in IP fabric when there is a change in the underlay network Product-Group=junos	On Junos QFX5K series, EX4400 platforms, configuration-change/protocol flapping/port flapping in Ethernet Virtual private network (EVPN) Virtual Extensible LAN (VXLAN) can cause traffic loss (changes related to the underlay network). *Resolved In:* junos:20.4R3-S7 junos:21.2R3-S5 junos:21.4R3-S4 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3 junos:22.3R3-S1 junos:22.4R2-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1

1691417	When a new VLAN is added on trunk interfaces, the newly added VLAN member drops the traffic Product-Group=junos	On QFX5K platforms with Virtual Extensible VLAN (VXLAN) configuration, when a new Virtual Local Area Network (VLAN) is added to the trunk, it is not getting added and traffic loss will be seen on the newly VLAN added port. *Resolved In:* junos:21.2R3-S4 junos:21.2R3-S5 junos:21.3R3-S3 junos:21.3R3-S4
1738276	High convergence time in the EVPN-VxLAN uplink failover scenario Product-Group=junos	On Junos QFX5K platforms in the EVPN-VxLAN scenario, due to high convergence time, traffic loss is more than expected when the uplink to the spine disabled (CLI initiated uplink failover). *Resolved In:* junos:20.4R3-S8 junos:21.2R3-S6 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.2R3-S3 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1-S2 junos:23.2R2 junos:23.3R1 junos:23.3R2 junos:23.4R1
1746460	The transit DHCP packets are getting dropped In a bridge (L2) overlay VXLAN network Product-Group=junos	Introduced via PR1636477, in an EVPN-VXLAN CRB architecture, the QFX5K/EX4K leaf switches that are running affected Junos software releases will drop all DHCP discover packets received on its data plane. This issue is applicable to all QFX5K platforms that support VXLAN L2 Gateway functionality such as QFX5100, QFX5110, QFX5120, QFX5200, QFX5210. No specific DHCP knob or DHCP-related configuration is needed on the CRB leaf device is trigger the problem. The impact of this issue can cause DHCP communication failure between DHCP clients and servers over VXLAN L2 VNI. The workaround is to configure IRB (on the EX/QFX platform that supports VXLAN routing) and retry to bind the DHCP clients. *Resolved In:* junos:21.4R3-S4 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: QFX5100 Interface related issues**
1665800	Ports with SFP-T 1G plugged in may go to hung state on QFX5100 platforms Product-Group=junos	When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission. *Resolved In:* junos:20.2R3-S7 junos:20.2R3-S8 junos:20.4R3-S6 junos:20.4R3-S7 junos:21.2R3-S3 junos:21.4R3-S3 junos:21.4R3-S4 junos:22.2R3-S1
PR Number	**Synopsis**	**Category: RPD Next-hop issues including indirect, CNH, and MCNH**
1716436	Traffic loss due to incorrect route resolution and KRT queue getting stuck with 'EINVAL -- Bad parameter in request' error Product-Group=junos	On all Junos and Junos OS Evolved platforms, due to a bug in route resolution over specific types of next hops, the route can resolve over itself and the nexthop chain keeps expanding. Due to this issue, the depth of recursion gets higher than supported and the KRT (Kernel Routing table) queue returns errors for nexthops. As a result, there will be incorrect route resolution, traffic loss and occasionally, the rpd (routing protocol deamon) crashes. The necessary configurations and conditions that will result in this issue are below 1. BGP (Border Gateway Protocol) Prefix-Independent Convergence (PIC) ("protect core") is configured and BGP receives same prefix from EBGP and IBGP neighbors 2. BGP LU (Labeled Unicast) with "protection" to create backup path to protect the active and BGP receives same prefix from EBGP and IBGP neighbors 3. Mutually recursive Route resolvability situations like Resolving using Default-route (not having proper resolution config) *Resolved In:* evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1
PR	**Synopsis**	**Category: RPD policy options**

Number		
1744449	Policy change to a rib-group import-policy configured with global routing-options interface-routes causes the rpd issue on all platforms with EVPN-VXLAN configuration Product-Group=junos	When a user configures "set routing-options interface-routes rib-group " along with an import policy for that particular rib-group, it will result in an unexpected behavior. It could disrupt the rpd or result in the rpd running at 100%. This issue is only related the "interface-routes" being configured in the global routing-options hierarchy with EVPN-VXLAN configuration. This issue won't be seen when routing-options configurations can have "interface-routes" enabled under specific routing instance. *Resolved In:* evo:21.2R3-S6-EVO evo:21.4R3-S5-EVO evo:22.1R3-S4-EVO evo:22.2R3-S2-EVO evo:22.3R3-S1-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:21.2R3-S6 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: RPD route tables, resolver, routing instances, static routes**
1716153	Multipath route is not getting compute and skip the multipath eligibility check Product-Group=junos	On all Junos platforms, multipath route will not be formed correctly when a BGP route is received from RR (Route Reflector) and preference decided based on cluster list length. *Resolved In:* evo:21.2R3-S6-EVO evo:21.4R3-S4-EVO evo:22.1R3-S3-EVO evo:22.2R3-S1-EVO evo:22.3R2-S2-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:23.1R1-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:20.3X75-D52 junos:21.2R3-S6 junos:21.4R3-S4 junos:22.1R3-S3 junos:22.2R3-S1 junos:22.3R2-S2 junos:22.3R3 junos:22.4R1-S2-J2 junos:22.4R2 junos:22.4R3 junos:23.1R1 junos:23.1R2 junos:23.2R1 junos:23.3R1
1742147	Memory leak observed when reconfiguring the flow routes Product-Group=junos	On all Junos and Junos OS Evolved platforms, if the nexthop of a flow route is the same as it was before when reconfiguring flow routes, memory leak occurs. High memory use of routing process daemon(rpd) is seen as a result of this leak. A kernel out of memory message is observed which results BGP flap. *Resolved In:* evo:21.2R3-S6-EVO evo:21.4R3-S5-EVO evo:22.1R3-S4-EVO evo:22.2R3-S2-EVO evo:22.3R3-S1-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-S1-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:20.4R3-S8 junos:21.2R3-S6 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: Resource Reservation Protocol**
1685182	RSVP path tear is not encapsulated by the MPLS header when bypass is configured Product-Group=junos	On all Junos and Junos Evolved platforms, RSVP(Resource Reservation Protocol) path tear is not encapsulated by the MPLS(Multiprotocol Label Switching) header, when "no-enhanced-frr-bypass" is configured on the routers that undertake FRR(fast re-route) procedures after the failure. *Resolved In:* evo:21.2R3-S3-EVO evo:21.3R3-S3-EVO evo:21.4R3-EVO evo:22.1R3-EVO evo:22.2R2-EVO evo:22.2R3-EVO evo:22.3R2-EVO evo:22.4R1-EVO junos:20.3X75-D43 junos:20.4R3-S9 junos:21.2R3-S3 junos:21.3R3-S3 junos:21.4R3-S1 junos:22.1R3 junos:22.2R2 junos:22.2R3 junos:22.3R2 junos:22.4R1
PR Number	**Synopsis**	**Category: PTX10K specific platform PRs**
1735224	Junos OS Evolved: PTX10001, PTX10004, PTX10008, PTX10016: MAC address	An Origin Validation vulnerability in MAC address validation of Juniper Networks Junos OS Evolved on PTX10001, PTX10004, PTX10008, and PTX10016 devices allows a network-adjacent attacker to bypass MAC address checking, allowing MAC addresses

	validation bypass vulnerability (CVE-2023-44190) Product-Group=junos	not intended to reach the adjacent LAN to be forwarded to the downstream network. Due to this issue, the router will start forwarding traffic if a valid route is present in forwarding-table, causing a loop and congestion in the downstream layer-2 domain connected to the device. Please refer to https://supportportal.juniper.net/JSA73154 for more information. *Resolved In:* evo:20.4X6-EVO evo:21.4R3-S5-EVO evo:22.1R3-S4-EVO evo:22.3R2-S2-EVO evo:22.3R3-S1-EVO evo:22.3X50-EVO evo:22.3X80-D35-EVO evo:22.3X80-D36-EVO evo:22.3X80-D37-EVO evo:22.4R2-S1-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-S1-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: Generic platform and infra issues for MS-MIC and MS-MPC(XLP)**
1700462	mspmand 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. mspmand is one of the processes inside PIC, crashes sometimes. *Resolved In:*
1743031	The picd process crashes when executing the CLI command "show service sessions/flows" or "clear service sessions/flows" Product-Group=junos	On MX platforms with MS-MPC/MS-DPC, when the system is busy in the creation/deletion of sessions results in the picd process crashes for executing the CLI command "show service sessions/flows" or "clear service sessions/flows" aggressively (executing CLI command in 5-10 secs iteration). *Resolved In:* evo:24.1R1-EVO junos:21.2R3-S4-J31 junos:21.2R3-S7 junos:22.4R3
PR Number	**Synopsis**	**Category: Remote Access VPN issues on SRX**
1671456	Juniper Secure Connect: Client build later than version 22.4.13.10 and Build: 29408 cannot connect to some Junos versions. Product-Group=junos	Customers on the Junos 20.4 release or prior should continue to use Juniper secure connect version 22.4.13.10 and Build: 29408 and below Customers on the following Junos build can upgrade to any Juniper Secure Connect client version 21.2R3-S3 21.4R3 22.1R3 22.2R2 22.3R1 22.4R1 and later *Resolved In:* junos:21.2R3-S3 junos:21.4R3 junos:22.1R3 junos:22.2R2 junos:22.3R1 junos:22.4R1
PR Number	**Synopsis**	**Category: ZT/YT pfe l3 forwarding issues**
1708283	Cosmetic logs may appear on MX platforms during ISSU Product-Group=junos	On MX platforms during ISSU (In-Service-Software-Upgrade) logs like the following may be seen: "marrow fpcx issu_stats_save: Failed to create counters for Tag = 23, Key = IFL_FC_CNTR_STATS:(345,16) xe-x/x/x.xxx, status = invalid argument?. These logs do not have any service impact. *Resolved In:* evo:23.2R1-EVO junos:23.2R1
PR Number	**Synopsis**	**Category: Trio LU, IX, QX, MQ chip drivers, ucode & related SW**
1648473	The FPC crash might be observed during ISSU Product-Group=junos	On all Junos platforms with scaled environment equipped with specific line cards like MPC7E/MPC8E/MPC9E etc., when there are memory errors, the FPC crash might be observed. This happens during ISSU (In-service software upgrade). *Resolved In:* evo:21.3R3-EVO evo:21.4R2-EVO evo:22.1R2-EVO evo:22.2R1-EVO junos:20.2R3-S5 junos:20.4R3-S5 junos:21.1R3-S5 junos:21.2R3 junos:21.3R2-S1 junos:21.3R3 junos:21.4R2 junos:22.1R1 junos:22.1R2 junos:22.2R1

PR Number	Synopsis	Category: Trio pfe qos software
1726698	On certain Junos MX platforms queue buffer-size temporal computation is not happening correctly Product-Group=junos	On certain Junos MX platforms, if a queue's buffer size is configured as temporal value and the transmit-rate/guaranteed-rate is not configured as absolute value at COS (Class of Service) schedulers or traffic-control-profile level, then a very low queue depth buffer gets allocated to the queue. This will lead to aggressive tail-drops on the queue. *Resolved In:* evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:22.3R3 junos:22.3R3-S2 junos:22.4R2-S2 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
PR Number	**Synopsis**	**Category: Trio pfe stateless firewall software**
1742123	Inline-monitoring will not work as expected when more than one instances are configured Product-Group=junos	On all Junos MX and EX9200 platforms, when more than one instances of the "inline-monitoring" service are placed under firewall filter, all prefixes point to the firewall filter first term regardless of the match condition which results in inline-monitoring not working as expected. *Resolved In:* evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:20.3X75-D46 junos:21.2R3-S4-J24 junos:21.2R3-S6 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: Trio pfe bridging, learning, stp, oam, irb software**
1720772	VLAN rewrite will not work for traffic egressing on IRB over L2 AE IFL Product-Group=junos	On Junos MX and EX92XX with specific line cards, VLAN rewrites will not happen for traffic egressing from IRB(Integrated Routing and Bridging) interface over an L2 AE (Aggregated Ethernet) IFL (Interface Logical), if the L2 AE IFL is configured to perform VLAN rewrites on the frames. This happens when the IRB is configured as a routing-interface on EVPN (Ethernet Virtual Private LAN) or VXLAN (Virtual Extensible LAN) routing instances and the traffic has to egress on IRB over an L2 AE IFL. As a result, the frames are forwarded with incorrect VLAN tag information. *Resolved In:* evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:21.2R3-S6 junos:21.4R3-S5 junos:22.2R3-J4 junos:22.2R3-S1 junos:23.1R2 junos:23.2R1 junos:23.3R1
1731564	VPLS traffic gets blackholed by qualified-bum-pruning mode Product-Group=junos	On all MX and EX9K platforms, qualified-bum-pruning-mode completely blackholes VPLS (Virtual Private LAN Service) traffic with network-services configured in enhanced-ip mode. *Resolved In:* evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:20.4R3-S7-J1 junos:20.4R3-S8 junos:21.2R3-S6 junos:21.4R3-S5 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: Trio pfe l3 forwarding issues**
1739854	Major alarms will be observed on the FPC when ALB is enabled under AE interface Product-Group=junos	On Junos MX platforms with MPC2-MPC9 line cards configured with ALB (Adaptive Load Balancing) under AE (Aggregate Ethernet) interface and Network-Services IP mode, when the AE interface comes up initially or activating AE after deactivating, the error logs of "Bad JNH Write to unilist-selector" and "LUCHIP Uncorrectable ECC" would be observed. These errors will lead to major alarms on the FPC (Flexible PIC Concentrators) causing traffic impact.

		Resolved In: evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:20.4R3-S8 junos:21.2R3-S6 junos:21.2X33-J6 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: PTX/QFX100002/8/16 interface software**
1712007	The interface does not come up or keeps flapping Product-Group=junos	On Junos PTX10008/PTX100016 devices with LC1101/LC1102 line cards, any event that causes an interface state change can lead to interface flapping or the interface may not come back at all. This leads to traffic impact on that interface. *Resolved In:* junos:20.3X75-D44 junos:20.4R3-S4-J14 junos:20.4R3-S6-J4 junos:20.4R3-S7 junos:21.1R3-S5 junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S3 junos:22.1R3-S2 junos:22.1R3-S4 junos:22.2R3 junos:22.3R3 junos:23.1R1 junos:23.1R2 junos:23.2R1
PR Number	**Synopsis**	**Category: Xellent Platform issues**
1709817	Ports with QSA adapter are down Product-Group=junos	On Junos PTX1000 and PTX10002-60C/QFX10002-60C platforms, ports which use the QSA (QSFP-to-SFP Adapter) may not come up when running software version containing the fix for PR 1620527. *Resolved In:* junos:19.4R3-S13 junos:20.3X75-D44 junos:20.4R3-S7 junos:21.1R3-S5 junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S3 junos:22.1R3-S2 junos:22.2R3 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.1R2 junos:23.2R1
PR Number	**Synopsis**	**Category: Express ZX PFE L3 Features**
1732283	Junos OS Evolved: PTX10003 Series: MAC address validation bypass vulnerability (CVE-2023-44189) Product-Group=junos	An Origin Validation vulnerability in MAC address validation of Juniper Networks Junos OS Evolved on PTX10003 Series allows a network-adjacent attacker to bypass MAC address checking, allowing MAC addresses not intended to reach the adjacent LAN to be forwarded to the downstream network. Due to this issue, the router will start forwarding traffic if a valid route is present in forwarding-table, causing a loop and congestion in the downstream layer-2 domain connected to the device.Please refer to https://supportportal.juniper.net/JSA73153 for more information. *Resolved In:* evo:21.4R3-S4-EVO evo:21.4X1-EVO evo:22.1R3-S3-EVO evo:22.3R2-S2-EVO evo:22.3R3-S1-EVO evo:22.3X50-EVO evo:22.3X80-D35-EVO evo:22.4R2-S1-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:22.3R2-S2 junos:22.3R3-S1 junos:22.4R2-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: usf ams related issues**
1738300	Eventd running 100% cpu cycle while running AMS statistics related show command continuously Product-Group=junos	On all Junos and Junos Evolved platforms, When 'show interfaces AMS' is executed continuously via CLI or SNMP, eventD spikes. This will not cause any impact. *Resolved In:* evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:21.2R3-S6 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: usf ipsec related issues**

1744601	With multiple Traffic Selectors having same remote-ip, the traffic works only for first tunnel on MX platforms with SPC3 cards Product-Group=junos	In MX-SPC3 IPSec deployments, if multiple traffic selectors are configured with same remote-ip (different local-ip), the traffic works only for one of the tunnels. *Resolved In:* junos:21.2R3-S6 junos:22.1R3-S4 junos:22.2R3-S2 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: usf nat related issues**
1612555	The B4 client traffic will be dropped on MX-SPC3 based AFTR in DS-Lite with EIM activated CGNAT scenario Product-Group=junos	In MX-SPC3 with Dual-Stack Lite (DS-Lite) scenario, the IPv4 client will use Basic Bridging BroadBand (B4) to pass through IPv4-over-IPv6 tunnels to cross an IPv6 access network to reach a Carrier-grade NAT (CGNAT) network behind the Address Family Transition Router (AFTR). In case of the Endpoint independent mapping (EIM) is activated for CGNAT, the DS-Lite encapsulated IPIP packets might not be identified by EIM for some reason, and the NAT rule might not be found properly by MX-SPC3 of AFTR for the mapping traffic. After that, the DS-Lite tunnels/NAT sessions between the B4 and AFTR might not be established successfully since the DS-Lite/NAT packets might be dropped on AFTR, the IP flow from the B4 client will be impacted. *Resolved In:* junos:20.2R3-S3 junos:20.4R3-S1 junos:21.1R2-S1 junos:21.1R3 junos:21.2R2 junos:21.2R3 junos:21.3R2 junos:21.4R1 junos:22.1R1