Juniper Networks | Engineering Simplicity

Juniper Networks® CTPView Server Software Release 9.3R3

Published
2026-06-05

RELEASE

Table of Contents

About This Guide

This release notes accompany Release 9.3R3 of the CTPView software. They describe device documentation and known problems with the software.

You can also find these release notes on the Juniper Networks CTP software documentation webpage, which is located at CTP Series Release Notes.

Release Highlights

The following features or enhancements have been added in CTPView Release 9.3R3.

- CTP upgrade archive dual img files specify the supported build.
- We have added backup/restore script for ctpview 9.3.
- Several reported low, high, medium and critical CVEs are fixed in this build.

Resolved Issues in CTPView Release 9.3R3

The following issues have been resolved in CTPView Release 9.3R3.

- CTPView NTP Server Admin config and connection issue. [PR 1906823]
- syslog messages are missing on latest CTPView. [PR 1908839]

  See PR details for workaround.
- NetMon will stops immediately when started. [PR 1939077]

  CTPView 9.3Rx root password expiry.
- CTP software upgrade status is not displayed in CTPView Upgrade CTP software page although CTP Node gets successfully upgraded. [PR 1872602]
- 9.3 upgrading issues using CTPView. [PR 1927424]
- CTP upgrade archive dual img files need to specify the supported build. [PR 1924915]
- Need backup/restore script for ctpview 9.3. [PR 1930060]

- Several Crit and high CVEs CTPView. [PR 1946632]
- CTPView 9.3R2-2 running on ROCKY Linux version 9.5 ACAS results shows several HIGH and Medium findings. [PR 1931100]
- CVE-2026-31431 copy fail vulnerability. [PR 1954063]

  See PR details for workaround.
- "dirty frag" vulnerability.[PR 1955675]
- Add support for more special characters in postgresql CTPView. [PR 1916509]

Known Issues in CTPView Release 9.3R3

The following PRs are known issues.

- /var is 100% full [PR 1927137]
- Server diags screen nogt accurate [PR 1927130]
- CTPView RHEL VM would not boot unless Secure boot disabled. [PR 1920986]
- Can't install CTPView 9.3R2-1 on ESXi-7.0U2a with EFI secure boot enabled. [PR 1900433]
- Need to support "dnf update" [PR 1942491]
- CTP upgrades need to be simplified and easier to perform [PR 1884638]
- Need to be able to support versions between CTPViews to migrate existing ctp data and configuration from 9.1x to 9.3x [PR 1946238]
- Upgrade to CTPOS 9.1R6x via CTPView fails on the Gen4 CTP2000 with an FXS card [PR 1942084]
- CTPView failing to upgrade CTP using single archive on CTP151 / CTP2000 nodes and dual archive not working on CTP2000 node [PR 1961454]
- CTPView save and restore CTP configuration except bundle unable to restore other configurations and Support more special characters in postgresql CTPView two password format is unable to add. [PR 1961510]
- Implement of CTPView Serial encoding of TDM functionality [PR 1907111]

NOTE: You cannot configure PBS in CTPView 9.3R3.

Required Install files

It is your responsibility to install either the RHEL9.5 (licensed version) or Rocky Linux 9.5 (open source) OS for hosting CTPView 9.3R3 Server.

If you have queries or need further assistance, contact Juniper Networks Technical Assistance Center (JTAC).

Following file is provided for installing the CTPView software:

Table 1:

File	CTPView Server OS	Filename	Checksum
Software and RHEL9.5 (licensed version) or Rocky Linux 9.5 (open source) OS updates	RHEL9.5 (licensed version) or Rocky Linux 9.5 (open source) OS	CTPView-9.3R-3.0.el9.x86_64.rpm tcsh-6.22.03-6.el9.x86_64.rpm	7bd31cb3a813c12f1bd4dec27e5bb664 57e999d72a82faa663ad65d60d1dd941

Recommended System Configuration for Hosting a CTPView Server

The following are the recommended hardware configuration to setup a CTPView 9.3R3 server:

- RHEL9.5 (licensed version) or Rocky Linux 9.5 (open source) OS
- 1x processor (4 cores)
- 8 GB RAM
- Number of NICs – 2

- 80 GB Disk space

CTPView Installation and Maintenance Policy

From the release of CTPView 9.0R1, Juniper Networks has adopted a policy for installation and maintenance of the CTPView server. CTPView is now being distributed as an "Application only" product, in the form of an RPM package. You can now install and maintain the OS (RHEL 9.5 or Rocky Linux 9.5) according to the guidelines described in Installing CTPView 9.3R1 Server Operating System and CTPView Network Management System Software. This administration guide also has the complete installation procedure.

NOTE:

- Starting from CTPView 9.3R1, you must use either RHEL 9.5 (licensed) or Rocky Linux 9.5 (open source) OS to host CTPView server.
- When RPM update is required due to vulnerability reported by scanner, it is your responsibility to download RPM from RHEL9 / Rocky Linux 9 vault **https://dl.rockylinux.org/vault/rocky/9.5/BaseOS/x86_64/os/Packages/** and install the latest update of the specific RPM in CTPView server.

  CTPView maintenance updates mandate, and possibly provide, up-to-date RPMs in every release.

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.3R3

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.3R3. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search.

Table 2: List of CVEs

CVEs List	
CVE-2026-1519	CVE-2025-11083

Table 2: List of CVEs *(Continued)*

CVEs List	
CVE-2025-67873, CVE-2025-68114	CVE-2026-30892
CVE-2025-59032, CVE-2026-27857, CVE-2026-27858	CVE-2025-45582
CVE-2025-59375	CVE-2025-9086
CVE-2026-5201	CVE-2026-23868
CVE-2025-14087, CVE-2025-14512	CVE-2025-15281, CVE-2026-0861, CVE-2026-0915
CVE-2026-34982	CVE-2025-68973
CVE-2025-61662	CVE-2026-25679
CVE-2025-58098, CVE-2025-65082, CVE-2025-66200	CVE-2025-48964
CVE-2025-38109, CVE-2026-23111, CVE-2026-23210, CVE-2026-23231	CVE-2026-4424, CVE-2026-5121
CVE-2025-14104	CVE-2025-6176
CVE-2026-4878	CVE-2025-11561
CVE-2026-27135	CVE-2026-33636
CVE-2025-12818	CVE-2025-5987
CVE-2026-4775	CVE-2025-8067
CVE-2025-9714	CVE-2023-40403
CVE-2025-68615	CVE-2026-1642

Table 2: List of CVEs *(Continued)*

CVEs List	
CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-15469, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796	CVE-2026-41651
CVE-2025-6020, CVE-2025-8941	CVE-2006-10002, CVE-2006-10003
CVE-2025-32365	CVE-2026-0994
CVE-2026-4786, CVE-2026-6100	CVE-2026-33186
CVE-2025-10158	CVE-2024-56433
CVE-2025-6965	CVE-2026-35535

Revision History

June 2026—Revision 1—CTPView Release 9.3R3