Engineering
Simplicity

Juniper Networks® CTPView Server Software Release 9.3R2

Published
2025-03-26

RELEASE

Table of Contents

About This Guide

Release Highlights

Resolved Issues in CTPView Release 9.3R2

Known Issues in CTPView Release 9.3R2

Required Install files

Recommended System Configuration for Hosting a CTPView Server

CTPView Installation and Maintenance Policy

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.3R2

Revision History

About This Guide

This release notes accompany Release 9.3R2 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 to CTPView Release 9.3R2.

- You can now host CTPView 9.3R2 Server on RHEL9 or Rocky Linux9 instead of Centos 7.
- You can now check FIPS 140-3 compliance in CTPView 9.3Rx [PR 1868120].

Resolved Issues in CTPView Release 9.3R2

The following issues have been resolved in CTPView Release 9.3R2.

- Security vulnerabilites in CTPView 9.3R1 [PR 1867535]

Known Issues in CTPView Release 9.3R2

The following PRs are known issues.

- SSH fails after CTP151 dual upgrade to CTPOS 9.2R1 from CTPView. [PR 1830027]
- Add support for more special characters in CTPView GUI system configuration page for various CTP applications [PR 1847606]
- CTP software upgrade status is not displayed in CTPView Upgrade CTP software page although CTP Node gets successfully upgraded [PR 1872602]

NOTE: You cannot configure PBS in CTPView 9.3R2.

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 9.3R2 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-2.0.el9.x86_64.rpm	0f37fd7b02cc5a9beaed0c6929229bc9

Recommended System Configuration for Hosting a CTPView Server

The following are the recommended hardware configuration to setup a CTPView 9.3R2 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 9.3R2

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.3R2. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search.

Table 2: Critical or Important CVEs Included in kernel

CVE-2024-53104	CVE-2024-53104	CVE-2023-52605
CVE-2023-52922	CVE-2024-50264	CVE-2024-50302
CVE-2024-53113	CVE-2024-53197	

Table 3: Critical or Important CVEs Included in libxml2

CVE-2022-49043	CVE-2022-49043	CVE-2024-56171
CVE-2025-24928		

Table 4: Critical or Important CVEs Included in openssh

CVE-2025-26466

Table 5: Critical or Important CVEs Included in bind

CVE-2024-11187

Table 6: Critical or Important CVEs Included in emacs-filesystem

CVE-2025-1244

Table 7: Critical or Important CVEs Included in openssl

CVE-2024-12797

Table 8: Critical or Important CVEs Included in grub2

CVE-2025-0624

Revision History

March 2025—Revision 1—CTPView Release 9.3R2