Juniper Networks | Engineering Simplicity

Juniper Networks® CTPView Server Software Release 9.2R1

Published
2024-08-13

RELEASE

Table of Contents

About This Guide

This release notes accompany Release 9.2R1 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 9.2R1.

- CTPOS Release 9.2R1 is supported on CTP151 device only.

You can upgrade to CTPOS 9.2R1 dual image from CTPOS 9.1R1/9.1R2/9.1R3-x/9.1R5/9.1R6-x using CTPView.

Table 1: CTPOS Upgrade Path

Model / Platform	Existing CTPOS Version	Version Path
CTP151	9.1R1/9.1R2/9.1R3-x/ 9.1R5/9.1R6-x	9.1R1/9.1R2/9.1R3-x/ 9.1R5/9.1R6-x> 9.2R1

- **Upgrading the dual image using CTPView 9.2R1**

  1. To upgrade from CTPView, copy `ctp_complete_9.2R1_240809.tgz` in **/ctp** of CTPView 9.2R1.
  2. Select **Node Maintenance > Upgrade CTP Software**.

> **NOTE**: After you dual upgrade your CTP151 node to CTPOS 9.2R1 from CTPView, SSH to CTP Node will not work. [PR 1830027].
>
> Workaround: Either reboot CTP151 node again or go to CTPOS CLI menu in the console and change the IP configuration to `eth4`.

Resolved Issues in CTPView Release 9.2R1

The following issues have been resolved in CTPView Release 9.2R1.

- Start using OpenSSL 3.0 [PR 1580060]
- Need to support TLS 1.3 [PR 1626634]
- The /var/www/ partition becomes 100% full. [PR 1627434]
- Update zlib to address CVE-2018-25032. [PR 1658343]
- Need instructions for renewing CTPView Self Cert. [PR 1670216]
- Error when submitting node config. [PR 1695689]
- Buffer stats port files grow huge and fill up /var/www/ [PR 1716742]
- Bundle config change freezes GUI screen. [PR 1727332]
- CTPView should prevent old 7.3 configs from being restored to a 9.1 CTP. [PR 1730056]
- CTPView CVE hotfix needed. [PR 1732911]
- Error when submitting CESoPSN Bundle on FXS port with multiple channels attached from CTPView. [PR 1733949]
- Radius SSH login does not roll back to local auth in 9.1R3.1. [PR 1737280]
- Add support for Ext Ref 10MHz in 9.x release in CTPView Node Synchronization page. [PR 1737507]
- GUI access denied CTPView 9.1R3.1 Server-Cert is expired. [PR 1740443]
- Hotfix versions need to be listed with the CTPView version. [PR 1740796]
- Some CTPView Netmon screens not populating. [PR 1749436]
- Penetration Test: Unauthenticated OS Command Injection and SQL Injection found in CTPView. [PR 1750343]
- Penetration Test: Excessive privileges given to Postgres SQL user and /etc/sudoers configuration file in CTPView. [PR 1750345]
- Remove yum command on CTPView. [PR 1755263]
- CTP groups may be empty when huge port issue happens. [PR 1758167]
- Add support of CTP Node upgrade from CTPView using acorn_310_9.1Rx_xxxxxx.tgz. [PR 1766296]

- CTPView_9.1R5 RPM not getting installed properly on Centos7. [PR 1766787]
- Penetration Test: CTPView has SELinux disabled and missing CSP Header. [PR 1775838]
- Not able to configure bundles on M/S ports of NPI SE cards. [PR 1781039]
- Penetration Test: CTPView has Debug code, verbose server headers, missing CSRF and arbitrary files are created during directory traversal. [PR 1783061]
- Penetration Test: Cookie discloses full application path and lacks Samesite Attribute. [PR 1783064]
- CTPView_9.1R6 upgrade using RPM package fails on 9.1R5 CTPView systems. [PR 1783448]
- CTPView: Code merge from 9.1x to 10.x [PR 1820891]
- CVE-2024-6387 - OpenSSH Remote Code Execution (RCE) [PR 1821683]
- Nessus scan vulnerabilities : Kernel, Linux-firmware, Postgresql. [PR 1821688]
- OpenSSH Vulnerability (CVE-2024-6387) [PR 1821690]
- SAToP interop with Cisco (matching source / destination UDP port) field needs to be added in CTPView. [PR 1826284]
- Disable PBS fields in CTPView to prevent PBS crashes on disable on CTP 151 with 10.0R2. [PR 1826882]
- Need hotfix for CTPView vulnerabilities in 9.1R3 [PR 1827420]
- CTPView code changes from 10.0R2 to 9.2R1 [PR 1829082]

Known Issues in CTPView Release 9.2R1

The following PR is a known issue.

- SSH fails after CTP151 dual upgrade to CTPOS 9.2R1 from CTPView. [PR 1830027]

Required Install files

It is your responsibility to install CentOS on a VM, and the CentOS version must be 7.5.1804 (http://vault.centos.org/7.5.1804/isos/x86_64/).

Installing newer releases of Centos are not supported you must use Centos 7.5.1804. 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 2:

File	CTPView Server OS	Filename	Checksum
Software and Centos OS updates	Centos 7.5	CTPView-9.2R-1.0.el7.x86_64.rpm	d7b1e282a0b2fbae963c805972e7933b
Web Update		web_update_9.2R1_240805.tgz	2a5c039d6137385df55d716cfcbd7da7

Recommended System Configuration for Hosting a CTPView Server

The following are the recommended hardware configuration to setup a CTPView 9.2R1 server:

- CentOS 7.5.1804 (64-bit)
- 1x processor (4 cores)
- 4 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 (CentOS 7.5) according to the

guidelines described in CTPView Network Management System Administration. This administration guide also has the complete installation procedure.

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.2R1

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.2R1. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search.

Table 3: Critical or Important CVEs Included in bind

CVE-2023-3341	CVE-2023-4408	CVE-2023-50387	CVE-2023-50868

Table 4: Critical or Important CVEs Included in glibc

CVE-2024-2961	CVE-2024-33599	CVE-2024-33600	CVE-2024-33601	CVE-2024-33602

Table 5: Critical or Important CVEs Included in grub2

CVE-2022-2601

Table 6: Critical or Important CVEs Included in kernel

CVE-2023-3609	CVE-2023-32233	CVE-2023-35001	CVE-2023-42753

Table 7: Critical or Important CVEs Included in libssh2

CVE-2020-22218

Table 8: Critical or Important CVEs Included in linux-firmware

CVE-2020-12321	CVE-2023-20569	CVE-2023-20593	CVE-2023-20592

Table 9: Critical or Important CVEs Included in postgresql

CVE-2023-5869

Table 10: Critical or Important CVEs Included in python

CVE-2023-40217

Table 11: Critical or Important CVEs Included in openssh

CVE-2023-48795	CVE-2023-51384	CVE-2023-51385

Revision History

August 2024—Revision 1—CTPView Release 9.2R1