Juniper Networks | Engineering Simplicity

Juniper Networks® CTPView Server Software Release 9.1R5-1

Published
2024-09-18

RELEASE

Table of Contents

About This Guide

This release notes accompany Release 9.1R5-1 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 9.1R5-1.

NOTE:

- CTPOS 9.1R5-1 is CTP 151-specific. However, CTPView software can manage both CTP151 and CTP2000 Series devices, but note that version of the CTPOS image on CTP2000 Series devices must be less than CTPOS Release 9.1R5.
- You cannot use CTPView to perform the CTP Node upgrade from 9.1Rx to 9.1R5-1.

  However, you can manually upgrade from CTPOS 9.1Rx to 9.1R5-1 using CTPOS CLI. See Table 1 on page 2 of CTPView 9.1R5 Release Notes

- OpenSSH Vulnerability (CVE-2024-6387) is fixed. [PR 1821683]
- CTPView vulnerabilities that were found in 9.1R3 are addressed and fixed. [PR 1827420]
- Nessus scan vulnerabilities (Kernel, Linux-firmware, Postgresql) are fixed. [PR 1821688]

Resolved Issues in CTPView Release 9.1R5-1

The following issues have been resolved in CTPView Release 9.1R5-1.

- CVE-2024-6387 - OpenSSH Remote Code Execution (RCE) [PR 1821683]
- Need hotfix for CTPView vulnerabilities in 9.1R3 [PR 1827420]

- Nessus scan vulnerabilities : Kernel, Linux-firmware, Postgresql. [PR 1821688]

Known Issues in CTPView Release 9.1R5-1

None.

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 1:

File	CTPView Server OS	Filename	Checksum
Software and Centos OS updates This includes CTPView software and security updates.	Centos 7.5	CTPView-9.1R-5.1.el7.x86_64.rpm	14a9772e954ea5d79da55e19bd3839b1
Software updates This includes CTPView software.	Centos 7.5	web_update_9.1R5-1_240911.tgz	7af71dfae9d92efb12154dd2599fc1de

Recommended System Configuration for Hosting a CTPView Server

The following are the recommended hardware configuration to setup a CTPView 9.1R5-1 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 9.1R5-1

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.1R5-1. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search.

Table 2: Critical or Important CVEs Included in bind

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

Table 3: Critical or Important CVEs Included in glibc

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

Table 4: Critical or Important CVEs Included in grub2

CVE-2022-2601

Table 5: Critical or Important CVEs Included in kernel

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

Table 6: Critical or Important CVEs Included in libssh2

CVE-2020-22218

Table 7: Critical or Important CVEs Included in linux-firmware

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

Table 8: Critical or Important CVEs Included in postgresql

CVE-2023-5869

Table 9: Critical or Important CVEs Included in python

CVE-2023-40217

Table 10: Critical or Important CVEs Included in openssh

CVE-2023-48795	CVE-2023-51384	CVE-2023-51385	CVE-2024-6387

Table 11: Critical or Important CVEs Included in httpd

CVE-2024-40725	CVE-2024-39884	CVE-2024-40898

Revision History

September 2024—Revision 1—CTPView Release 9.1R5-1.