

Juniper Networks® CTPView Server Software Release 9.1R3.8

Published
2024-09-11

RELEASE

Table of Contents

About This Guide

Release Highlights

CTPView Installation and Maintenance Policy

Resolved Issues in CTPView Release 9.1R3.8

Known Issues in CTPView Release 9.1R3.8

Required Install files

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.1R3.8

Revision History

About This Guide

These release notes accompany Release 9.1R3.8 of the CTPView Server Software. They contain install information and describe the enhancements to the software. The CTPView Release 9.1R3.8 software is compatible with Juniper Networks CTP Series platforms running CTPOS versions 7.3R7-1, 7.3R8, 9.0R1, 9.1R1, 9.1R2 or 9.1R3-6 for the features supported on those releases.

NOTE: Release version *9.1R3.8* and *9.1R3-8* are interchangeable and synonymous.

You can also find these release notes on the Juniper Networks CTP Software Documentation webpage, which is located at https://www.juniper.net/documentation/product/en_US/ctpview.

Release Highlights

The following features or enhancements have been added to CTPView Release 9.1R3.8.

- CTPView vulnerabilities that were found in 9.1R3 are addressed and fixed.
- OpenSSH Vulnerability (CVE-2024-6387) is fixed.
- 4WEM signaling is now configurable from CTPView.

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.

Resolved Issues in CTPView Release 9.1R3.8

The following issues have been resolved in CTPView Release 9.1R3.8:

- Need hotfix for CTPView vulnerabilities in 9.1R3 [PR 1827420]
- CVE-2024-6387 - OpenSSH Remote Code Execution (RCE) [PR 1821683]
- 4WEM signaling is not configurable from CTPView - need a Hotfix [PR 1821682]

Known Issues in CTPView Release 9.1R3.8

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-3.8.el7.x86_64.rpm	66f16b1a76311e6d1b0b3a6974a61993

Table 1: (Continued)

File	CTPView Server OS	Filename	Checksum
This includes CTPView software.		web_update_9.1R3-8_240822.tgz	59537059e062fd0494c4c1eeaae02646

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.1R3.8

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.1R6-1. 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

August 2024—Revision 1—CTPView Release 9.1R3.8.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2024 Juniper Networks, Inc. All rights reserved.