

CTPView Management System 9.1R2

Software Release Notes

Release 9.1R2 December 2020

These release notes accompany Release 9.1R2 of the CTPView Management System software. They contain install information and describe the enhancements to the software. The CTPView Release 9.1R2 software is compatible with Juniper Networks CTP series platforms running CTPOS version 9.1R2 or earlier.

You can 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 9.1R2.

- [PR 1364238] STIG hardening for CTPView 9.1R2.
- [PR 1563701] Enable serial console by default when CTPView is installed on a Centos 7 physical server.

NOTE: CTPView 9.1R2 runs on an updated OS (CentOS 7.5.1804) which provides better security with improved resilience and robustness.

The following features are not supported in CTPView Release 9.1R2.

- [PR 1409289] PBS and L2Agg features are not supported. These features will be reintroduced in a future release.
- [PR 1409293] VCOMP bundle and CESoPSN analog voice bundle features are not supported. These features will be reintroduced in a future release.

Resolved Issues in CTPView Release 9.1R2

The following issues have been resolved in CTPView Release 9.1R2:

- [PR 1468711] CTPView 9.1R2 requires users to change the default password of default user accounts.

Known Issues in CTPView Release 9.1R2

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/). For information on how to create a CentOS 7 virtual machine, see “Creating a CentOS 7 Virtual Machine” on page 3. 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:

File	Filename	Checksum
Software and CentOS OS Updates	CTPView-9.1R-2.0-1.el7.x86_64.rpm	5e41840719d9535aef17ba275b5b6343

Use the following information to determine the correct file to use:

CTPView Server OS	Installed CTPView Release	File for Upgrade	Server Reboots During Upgrade?
CentOS 7.5	NA	CTPView-9.1R-2.0-1.el7.x86_64.rpm	Yes

Recommended System Configuration for Hosting a CTPView Server

The following are the recommended hardware configuration to setup a CTPView 9.1R2 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 new 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 "Installing CTPView 9.1R2" on page 8. With the CTPView 7.3Rx and earlier releases, the OS (CentOS 5.11) and CTPView application were combined and distributed as a single installation ISO, and all updates (OS and CTPView application) were only available from Juniper Networks. This causes a delay in getting CTPView maintenance releases for important security updates (including Linux OS applications and CTPView application).

With this new model, you can update individual CentOS applications independently from the CTPView application if any security vulnerabilities are reported for the Linux OS applications. This provides more flexibility you need to ensure the security of your Linux-based platforms.

CTPView is made up of:

- Type 1—Stock CentOS 7.5 RPMs
- Type 2—Stock CentOS RPMs from other CentOS versions
- Type 3—Modified CentOS RPMs
- Type 4—CTPView application file

Where, "Stock" RPMs are the packages that are associated with a particular release of CentOS and readily available on the Internet. "Modified" RPMs are stock versions of RPMs that are modified by Juniper Networks for the needs of the CTPView platform. The CentOS 7.5 installation ISO only contains the components of type 1. The monolithic CTPView RPM contains the remaining components of types 2, 3, and 4, which can be unpacked and installed.

When Juniper Networks delivers a CTPView maintenance release RPM, it contains the updated component versions of types 2, 3, and 4. It also contains dependencies to make sure that type 1 components are also up to date and warn the user if any of them need to be updated.

Juniper Networks maintains a list of RPMs for CTPView that we suggest to be upgraded for security and functional reasons. The following methods are used for determining which CTPView RPMs need updates:

- Regular Retina/Nessus scans
- Notifications from Juniper's SIRT team
- Reports from customers

When an RPM update is required, Juniper Networks validates the new version of the component to make sure that it functions properly before adding it to the RPM list. This list will be shared to you via a KB. Although CTPView maintenance updates mandate (and possibly provide) up-to-date RPMs before installation, this RPM list helps you to update your CTPView software between releases. If there is an RPM added to the RPM list, you can take immediate action. Juniper Networks delivers the components of type 3 via maintenance releases only. For type 1 and 2 components, the RPMs should be freely available on the web, and Juniper Networks provides sample links. If you discover that an RPM needs a security update and it is not in the RPM list, you can notify us so that we can test it and add it to the list.

CAUTION: A bulk RPM update using "yum update" is strictly forbidden. CTPView 9.x, although mainly based on CentOS 7.5, is also made up of RPMs from other distributions. Performing an update to the latest version of CentOS 7 may cause CTPView to be non-functional, and a reinstallation may be required.

If you update RPMs that are not on the KB RPM list, CTPView may not function properly.

Creating a Centos 7 Virtual Machine

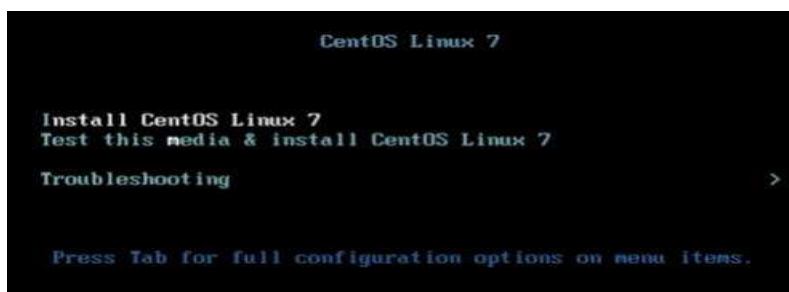
Before you begin:

- Make sure that vSphere client is installed on your workstation.

NOTE: Within vSphere, there are numerous ways to perform a particular task. The following example illustrates one such method. You can use the procedure that suits your network deployment effectively.

To create a new CentOS 7 STIG'd VM instance of CTPView server on an ESXi Server:

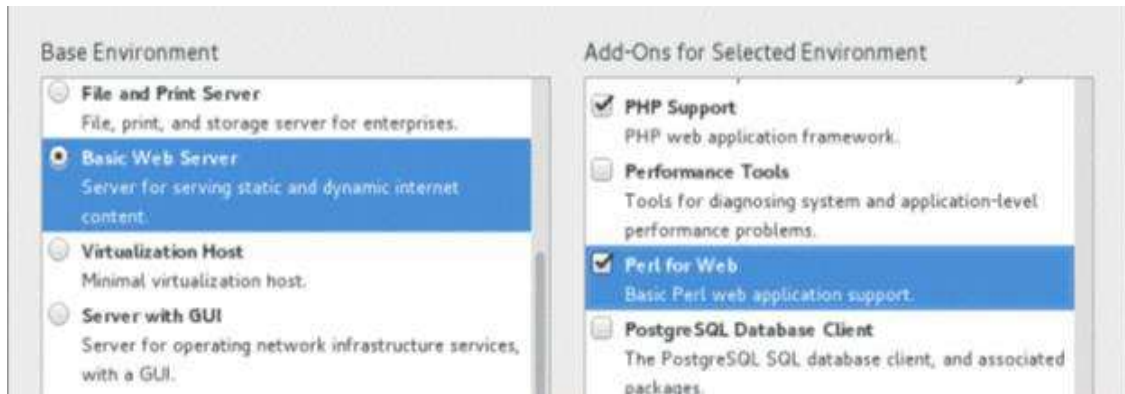
1. Copy the CentOS 7 ISO file (**centOS-7-x86_64-DVD-1804.iso**) to the ESXi datastore. The CentOS 7 ISO can be downloaded from http://vault.centos.org/7.5.1804/isos/x86_64/.
2. Start the vSphere client and enter the ESXi server IP address and your login credentials.
3. Start the wizard to create a new virtual machine. Select **File > New > Virtual Machine**.
4. Select the configuration as **Typical** and click **Next**.
5. Enter a name for the VM. For example, CTPView_9.1R2.
6. Select the datastore (with at least 80 GB free space) and click **Next**.
7. Select Guest OS as **Linux** and version as **Other Linux (64-bit)**, and then click **Next**.
8. Select the number of NICs as **2** and adapter type as **E1000**, and then click **Next**.
9. Select the virtual disk size as **80 GB** and select **Thick Provision Lazy Zeroed**.
10. Select the **Edit the virtual machine settings before completion** check box and click **Continue**.
11. Click the **Hardware** tab and select memory size as **4 GB**.
12. In the **Hardware** tab, select **CPU**. Then, select the number of virtual sockets as **2** and number of cores per socket as **1** (you can select up to 4 cores).
13. In the **Hardware** tab, select **CD/DVD**. Then, select the device type as **Datastore ISO File** and browse to CentOS 7 ISO file. Select the **Connect at power on** check box under **Device Status**.
14. Click **Finish**.
15. Select your created virtual machine in the left panel of **vSphere > Inventory**.
16. In the **Getting Started** tab, select **Power on the virtual machine**.
17. Switch to the **Console** tab and click inside the terminal emulator.
18. Select the **Install CentOS Linux 7** option with the Up-Arrow key and press **Enter**.



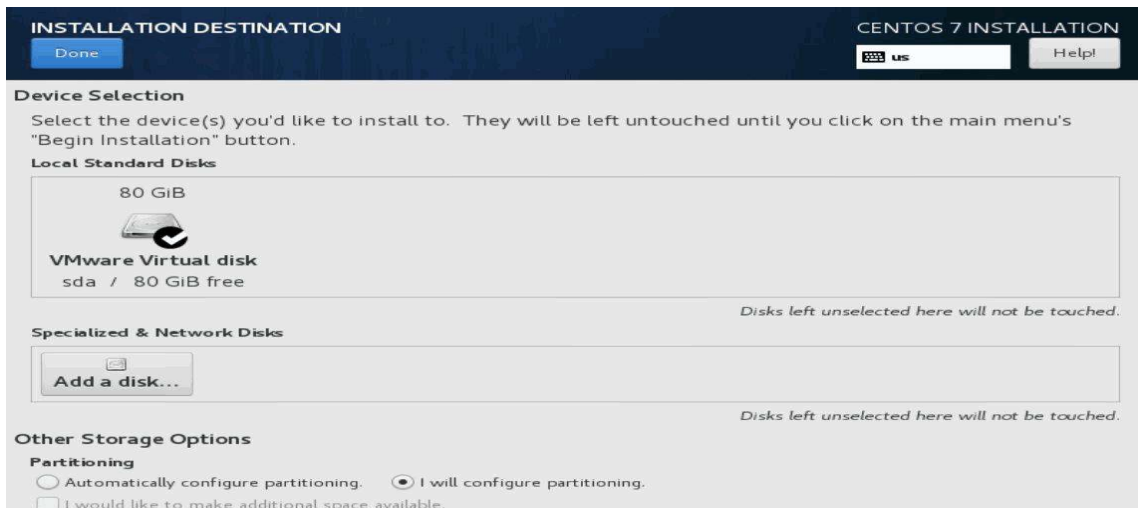
19. Press the **Enter** key to begin the installation process.
20. Select the language and your desired country time zone (if necessary) and then click **Continue**.
21. Click the **SOFTWARE SELECTION** option.



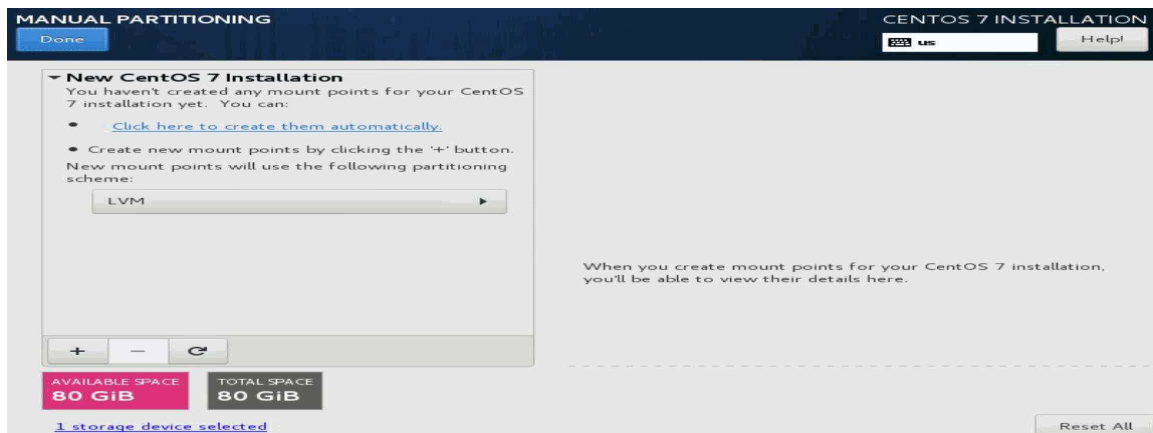
22. In the **Basic Environment** section, select the **Basic Web Server** radio button. In the **Add-Ons for Selected Environment** section, select **PHP Support** and **Perl for Web** check boxes and click **Done**.



23. Click **INSTALLATION DESTINATION** and verify that the **VMware Virtual disk (80 GB)** is selected.
24. In the **Other Storage Options** section, select the **I will configure a partitioning** option button.



25. Click **Done**. The **MANUAL PARTITIONING** page appears.



26. Click the **+** button. The **ADD A NEW MOUNT POINT** dialog box appears.

27. To create a partition for /boot, enter **/boot** in the **Mount Point** field and enter **1014 MB** in the **Desired Capacity** field. Then, click **Add mount point**.

ADD A NEW MOUNT POINT

More customization options are available after creating the mount point below.

Mount Point:

Desired Capacity:

28. Select **Standard Partition** from the **Device Type** list and select **ext3** from the **File System** list. Enter **LABEL=/boot** in the **Label** field and then click **Update Settings**.

New CentOS Linux 7 Installation

SYSTEM

/boot 967 MiB >

sda1

967 MiB

Device Type: ☐ Encrypt

File System: ☒ Reformat

Label: Name:

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

29. Similarly, repeat the steps 26 through 28 to create partitions for the following mount points with the provided settings.

Table 1: Mount Points and Their Settings

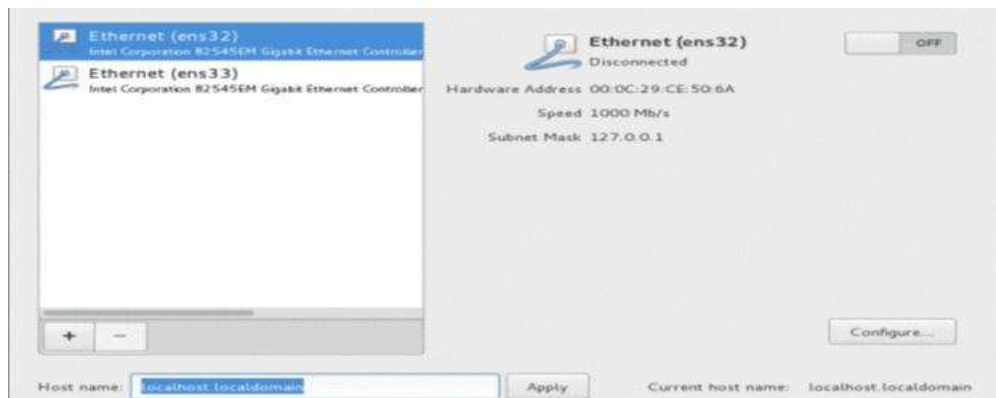
Mount Point	Desired Capacity	Device Type	File System	Label
/tmp	9.5 GB	Standard Partition	ext3	LABEL=/tmp
/	8 GB	Standard Partition	ext3	LABEL=/
/var/log	3.8 GB	Standard Partition	ext3	LABEL=/var/log
/var	3.8 GB	Standard Partition	ext3	LABEL=/var
/var/log/audit	1.9 GB	Standard Partition	ext3	LABEL=/var/log/a
/home	1.9 GB	Standard Partition	ext3	LABEL=/home
/var/www	9.4 GB	Standard Partition	ext3	LABEL=/var/www

30. Click **Done** twice and then click **Accept Changes**.



31. Click **NETWORK & HOST NAME**.

32. Select an Ethernet option (for example, Ethernet (ens32)), enter the hostname (for example, ctpview) in the **Host name** field, and then click **Apply**.



33. Click **Configure**. Then, click the **IPv4 Settings** tab.



34. Select **Manual** from the **Method** list and click **Add**.

35. Enter values for **Address**, **Netmask**, and **Gateway** fields, and then click **Save**.

36. Click the toggle button in the right-top corner to bring the configured Ethernet up and running, and then click **Done**.

37. Click **SECURITY POLICY**.

38. Select the **DISA STIG for CentOS Linux 7 Server** option and click **Select Profile**. Then, click **Done**.

39. Click **Begin Installation**. The **USER SETTINGS** page appears.

40. Click **USER CREATION**, enter the username as “admin”, and enter a password. Please don’t enter username as “juniper_sa” here.



41. Select the **Make this user administrator** check box and click **Done**.

42. In the **USER SETTINGS** page, click **ROOT PASSWORD**, enter the password as “CTPView-2-2” or any other password and click **Done**.

43. After the installation process is completed, click **Reboot**.

Installing CTPView 9.1R2

CTPView can be installed on the newly created CentOS 7.5[1804] VM or CentOS 7.5[1804] bare metal server. Steps are as follows:

1. Create a new CentOS 7 Virtual Machine (VM) instance as mentioned in “Creating a Centos 7 Virtual Machine” on page 3.
2. Copy the CTPView RPM (**CTPView-9.1R-2.0-1.el7.x86_64.rpm**) to /tmp directory of the newly created CentOS 7.5[1804] VM or CentOS 7.5[1804] bare metal.
3. Login as “admin” user that you created at the time of creating Centos 7 VM. Install CTPView RPM. If installing on top of
 - Centos 7 or 9.1R1 – use command “`sudo rpm -Uvh CTPView-9.1R-2.0-1.el7.x86_64.rpm`”
 - 9.0R1 – use command “`sudo rpm -Uvh --force CTPView-9.1R-2.0-1.el7.x86_64.rpm`”.
4. Change the passwords for all the default user accounts (juniper_sa, root, Juniper, ctpview_pgsql) at the end during upgrade (Refer section Change password of Default User accounts).

Change password of Default User accounts

This step is applicable only when you install CTPView 9.1R2 RPM on your server. Change the passwords for all the default user accounts as shown below:


```
#####
#####
CTPView has been installed on your system. Now, You need to set the passwords for all the default user accounts.
#####
#####
#####
#####
#####
#####
PLEASE REMEMBER THESE PASSWORDS!!!
```

Password recovery is not a simple process:

- It is service affecting.
- It requires console access to the CTPView
- It requires rebooting the CTPView (Possibly even a system repower)

```
#####
#####
#####
```

The new password must be alphanumeric or the characters

@ { } # % ~ [] = & , - _ !

The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Note : If unique passwords are not required, use "CTPView-2-2"

Enter New UNIX Password for root

Retype New UNIX Password for root

Changing password for user root.

passwd: all authentication tokens updated successfully.

This will be a System Administrator

The new password must be alphanumeric or the characters

@ { } # % ~ [] = & , - _ !

The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Note : If unique passwords are not required, use "CTPView-2-2"

Enter New UNIX Password for juniper_sa

Retype New UNIX Password for juniper_sa

Changing password for user juniper_sa.

passwd: all authentication tokens updated successfully.

The new password must be alphanumeric or the characters

@ { } # % ~ [] = & , - _ !

The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Note : If unique passwords are not required, use "CTPView-2-2"

Changing password for user Juniper

Enter the new password:

Re-Enter the new password:

You will now be asked for the password of the PostgreSQL Administrator account:

Password for user postgres:

==== Successfully updated the CTPView password for default user Juniper. =====

Note: The user Juniper has been assigned to the default user group TempGroup and has been given default user properties. Review the values using the CTPView Admin Center and make any appropriate modifications.

The new password must be alphanumeric or the characters

@ { } # % ~ [] = & , - _ !

The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Note : If unique passwords are not required, use "CTPView-2-2"

Changing password for user ctview_pgsql

Enter the new password:

Re-Enter the new password:

You will now be asked for the password of the PostgreSQL Administrator account:

Password for user postgres:

Note - You can also reset the password of all default user accounts from CTPView menu -> Advanced Functions
-> Reset account for default System Administrator

Uninstalling CTPView 9.1R2

CTPView 9.1R2 can be uninstalled from Centos 7 by performing the following steps:

1. Check if root login is permitted. If not, enable root login from menu -> Security Profile(1) -> Modify Security Level(5) -> Set OS level to 'very-low'(3).
2. Login via "root" user and run the command "sudo rpm -evh CTPView-9.1R-2.0-1.el7.x86_64".
3. System will reboot after uninstalling, use user (the one you created while creating CentOS 7) to login.

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.1R2

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.1R2.

For more information about individual CVEs, see <http://web.nvd.nist.gov/view/vuln/search>.

Table 2: Critical or Important CVEs Included in php

CVE-2018-10547	CVE-2018-5712	CVE-2018-7584	CVE-2019-9024
----------------	---------------	---------------	---------------

Table 3: Critical or Important CVEs Included in kernel

CVE-2019-14816	CVE-2019-14895	CVE-2019-14898	CVE-2019-14901
CVE-2019-17133	CVE-2019-11487	CVE-2019-17666	CVE-2019-19338
CVE-2015-9289	CVE-2017-17807	CVE-2018-19985	CVE-2018-20169
CVE-2018-7191	CVE-2019-10207	CVE-2019-10638	CVE-2019-10639
CVE-2019-11190	CVE-2019-11884	CVE-2019-12382	CVE-2019-13233
CVE-2019-13648	CVE-2019-14283	CVE-2019-15916	CVE-2019-16746
CVE-2019-18660	CVE-2019-3901	CVE-2019-9503	CVE-2020-12888
CVE-2017-18551	CVE-2018-20836	CVE-2019-9454	CVE-2019-9458
CVE-2019-12614	CVE-2019-15217	CVE-2019-15807	CVE-2019-15917
CVE-2019-16231	CVE-2019-16233	CVE-2019-16994	CVE-2019-17053
CVE-2019-17055	CVE-2019-18808	CVE-2019-19046	CVE-2019-19055
CVE-2019-19058	CVE-2019-19059	CVE-2019-19062	CVE-2019-19063
CVE-2019-19332	CVE-2019-19447	CVE-2019-19523	CVE-2019-19524
CVE-2019-19530	CVE-2019-19534	CVE-2019-19537	CVE-2019-19767
CVE-2019-19807	CVE-2019-20054	CVE-2019-20095	CVE-2019-20636
CVE-2020-1749	CVE-2020-2732	CVE-2020-8647	CVE-2020-8649
CVE-2020-9383	CVE-2020-10690	CVE-2020-10732	CVE-2020-10742
CVE-2020-10751	CVE-2020-10942	CVE-2020-11565	CVE-2020-12770
CVE-2020-12826	CVE-2020-14305	CVE-2019-20811	CVE-2020-14331

Table 4: Critical or Important CVEs Included in net-snmp

CVE-2018-18066

Table 5: Critical or Important CVEs Included in nss, nspr

CVE-2019-11729	CVE-2019-11745	CVE-2019-11719	CVE-2019-11727
CVE-2019-11756	CVE-2019-17006	CVE-2019-17023	CVE-2020-6829
CVE-2020-12400	CVE-2020-12401	CVE-2020-12402	CVE-2020-12403

Table 6: Critical or Important CVEs Included in python

CVE-2018-20852	CVE-2019-16056	CVE-2019-16935	CVE-2019-20907
----------------	----------------	----------------	----------------

Table 7: Critical or Important CVEs Included in OpenSSL

CVE-2016-2183

Table 8: Critical or Important CVEs Included in sudo

CVE-2019-18634

Table 9: Critical or Important CVEs Included in rsyslog

CVE-2019-17041	CVE-2019-17042
----------------	----------------

Table 10: Critical or Important CVEs Included in httpd

CVE-2017-15710	CVE-2018-1301	CVE-2018-17199
CVE-2017-15715	CVE-2018-1283	CVE-2018-1303
CVE-2019-10098	CVE-2020-1927	CVE-2020-1934

Table 11: Critical or Important CVEs Included in unzip

CVE-2019-13232

Table 12: Critical or Important CVEs Included in bind

CVE-2018-5745	CVE-2019-6465	CVE-2019-6477	CVE-2020-8616
CVE-2020-8617	CVE-2020-8622	CVE-2020-8623	CVE-2020-8624

Table 13: Critical or Important CVEs Included in curl

CVE-2019-5436	CVE-2019-5482	CVE-2020-8177
---------------	---------------	---------------

Table 14: Critical or Important CVEs Included in fribidi

CVE-2019-18397

Table 15: Critical or Important CVEs Included in expat

CVE-2018-20843	CVE-2019-15903
----------------	----------------

Table 16: Critical or Important CVEs Included in glib2

CVE-2019-12450	CVE-2019-14822
----------------	----------------

Table 17: Critical or Important CVEs Included in libpng

CVE-2017-12652

Table 18: Critical or Important CVEs Included in cpio

CVE-2019-14866

Table 19: Critical or Important CVEs Included in e2fsprogs

CVE-2019-5094	CVE-2019-5188
---------------	---------------

Table 20: Critical or Important CVEs Included in freetype

CVE-2020-15999

Table 21: Critical or Important CVEs Included in hunspell

CVE-2019-16707

Table 22: Critical or Important CVEs Included in libX11

CVE-2020-14363

Table 23: Critical or Important CVEs Included in libcroco

CVE-2020-12825

Table 24: Critical or Important CVEs Included in libssh2

CVE-2019-17498

Table 25: Critical or Important CVEs Included in openldap

CVE-2020-12243

Table 26: Critical or Important CVEs Included in dbus

CVE-2019-12749

Table 27: Critical or Important CVEs Included in glibc

CVE-2019-19126

Table 28: Critical or Important CVEs Included in systemd

CVE-2019-20386

CTP Documentation and Release Notes

For a list of related CTP documentation, see

https://www.juniper.net/documentation/product/en_US/ctpview

If the information in the latest release notes differs from the information in the documentation, follow the CTPoS Release Notes and the CTPView Server Release Notes.

To obtain the most current version of all Juniper Networks technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit-
<https://www.juniper.net/support/warranty/>
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Revision History

December 2020—Revision 1, CTPView Release 9.1R2

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.