Juniper Networks® CTPView Server Software Release 7.0R1 Release Notes

Release 7.0R1
September 2014
Revision 2

These release notes accompany Release 7.0R1 of the CTPView Server Software. They contain upgrade information and describe the enhancements to the software. The CTPView Release 7.0R1 software is compatible with Juniper Networks CTP Series platforms running CTPOS version 7.0 or earlier.

You can also find these release notes on the Juniper Networks CTP Software Documentation webpage, which is located at https://www.juniper.net/techpubs/en_US/ctp7.0/information-products/pathway-pages/ctp-series/index.html .

Contents

New Features

The following features have been added to CTPView Release 7.0R1.

Support for Analog CESoPSN Bundles over T1E1 on CTP2000 Devices

Starting from CTPView Release 7.0R1, the CTP2000 system supports analog CESoPSN bundles over T1E1, even if no VComp card is installed. To create an analog CESoPSN bundle, the T1E1 card must be installed in slot 0. If the T1E1 card is not installed in slot 0, the system displays the message **Analog Port CESoPSN Bundle will be created only when there is a T1E1 card present on slot 0**. The CTP2000 device supports a maximum of 16 analog CESoPSN bundles. [PR/947204]

Legacy (Non- analog) CESoPSN Bundle Configuration Limits on CTP2000 Devices

Starting from CTPOS Release 7.0R1, CTP2000 device supports a maximum of 16 CESoPSN Bundles on T1E1 Ports[0:3] and an additional 16 CESoPSN bundles on T1E1 Port[4:7] . CESoPSN bundles over T1E1 supports a maximum of 32 bundles per T1E1 card. Thus, the device supports a total of 64 bundles, which could be CTP, SAToP, CESoPSN, or VComp bundles.

Support for TRANS 8 Encoding from the CTPView Interface

Starting from CTPView Release 7.0R1, you can configure TRANS 8 encoding from the CTPView GUI. In earlier versions, you could configure TRANS8 only from the CTP Menu.

Support for Y-Cable Redundancy on T1E1 Ports on CTP2000

Starting from CTPView Release 7.0R1, CTP2000 devices support Y-cable redundancy on both serial and T1E1 interfaces. CTPOS Release 6.6 and earlier support Y-cable redundancy only on serial interfaces.

T1E1 ports support Y-cable redundancy by means of a software link. A software link does not require a Y cable. Y-cable port pairs maintain contact with each other by using the OAM packets that port pairs use to communicate with each other.

Enhancements to CESoPSN Bundle Query Output

CESoPSN bundle query output has been enhanced by including fields such as Last counter clear and Checked out PPS.

Security Enhancements to Operating System Applications

Table 1 on page 3 lists the CentOS applications that have been upgraded and their versions.

Table 1: Applications Upgraded for CentOS

Application	Upgraded Version
OpenSSL	0.9.8zb
NSS	nss-3.16.1-4.el5_11

Table 1: Applications Upgraded for CentOS *(continued)*

Application	Upgraded Version
NSPR	nspr-4.10.6-1.el5_10
PHP	php-5.3.27-2.centos53.jnpr
Kernel	2.6.18-371.1.2.el5
Oracle MySQL	mysql-5.1.66-2.centos53.jnpr
HTTPD	httpd-2.2.25-1
SudT	1.8.8
SOS	sos-1.7-9.62.el5_9.1
FreeType RPM	freetype-2.2.1-32.el5_9.1
LibPNG	1.2.10-17
krb5-libs RPM	krb5-libs-1.6.1-70.el5_9.2
glibc	glibc-2.5-107.el5_9.5
PAM	pam-0.99.6.2-12.el5
libxml	libxml2-2.6.26-2.1.21.3
BASH	3.2.33

NOTE: The updated RPM for BASH is bash-3.2-33.el5_10.4.i386.rpm. You can verify the successful installation of this RPM by using the **rpm –qa | grep bash** command. The expected output of this command is similar to **bash-3.2-33.el5_10.4**. This output displays the installed BASH RPM version in the CTPView server.

BASH contains the fixes for CVE-2014-6271 and CVE-2014-7169, which are also known as shellshock vulnerability fixes. You can use the **env x='() { :;}; echo vulnerable' bash -c "echo this is a test"** command to test the shellshock vulnerability fixes. The expected output of this command is **“this is a test”**. However, if the output of this command is **“vulnerable”**, then the shellshock vulnerability is not fixed in the CTPView server and the BASH package should be further upgraded.

Required Upgrade Files

The full suite of security enhancements is available only when the CTPView software is installed on servers running CentOS 5.3. Contact Juniper Networks Technical Assistance Center (JTAC) if you need to upgrade your operating system.

We provide the following files for upgrading the CTPView software:

- **web_update_7.0R1_140928.tgz** [software updates]
- **ctpview_complete_centos_7.0R1_140928.tgz** [software and CentOS OS updates]

The upgrade files that you use depend on the current CTPView server's operating system and the current CTPView software release. Use Table 2 on page 5 to determine the correct file to use.

Table 2: Determining the Required Upgrade Files for Your System

CTPView Server OS	Installed CTPView Release	File for Upgrade	Server Reboots During Upgrade?
CentOS 5.3	4.5R2 or earlier 4.6R1 or earlier	**ctpview_complete_centos_7.0R1_140928.tgz**	Yes

Upgrading the CTPView Software

These section describe how to upgrade CTPView Server Software to Release 7.0R1

This topic includes the following tasks:

Upgrading the CTPView Software for Systems Running Version 3.4R2-p1 or 3.4R3 or Later

This topic describes how to upgrade systems that run CTPView Server Software Release 3.4R2-p1 or 3.4R3 or later to CTPView Server Software Release 7.0

To install the CTPView Server oftware for systems running 3.4R2-p1 or 3.4R3 or later:

1. Use Secure Copy Protocol (SCP) to copy the **web_update** or **ctpview_complete** file to the **/tmp** directory on the server.
2. Log in to the server shell. On CentOS systems, log in as system administrator.
3. Run the installation script as root: **upgrade** or as system administrator: **upgrade**.

NOTE: When upgrading CentOS 5.3 systems running a release earlier than CTPView Release 4.2, you are prompted to enter the MySQL administrator's password. This password is needed to upgrade the database structures. If you do not enter the correct password, the upgrade process continues, but the server remains usable with limited MySQL functionality. In this case, to complete the upgrade process you need to manually initiate the database structure upgrade script from the CTPView CLI menu. The path to this function is **Menu** > **MySQL Functions** > **Upgrade Database Structures**.

Upgrading the CTPView Software for Systems Running Version 3.4R2 or Earlier

To install the CTPView software by using one of the **ctpview_complete** files:

1. Use SCP to copy the **ctpview_complete** file to the **/tmp** directory on the server.
2. Log in to the server shell and switch to the **root** user.
3. Unpack the archive.
4. Run the upgrade script: **upgrade**.

To install the CTPView software by using the **web_update** file:

1. Copy the upgrade file to the **/tmp** directory on the server.
2. Log in to the server shell and switch to the root user.
3. Run the upgrade installation script: **upgrade**.

Resolved Issues in CTPView Release 7.0R1

The following issues have been resolved in CTPView Release 7.0R1:

- CTPView must support CESoPSN bundles on analog ports on CTP2000 devices. [PR/947204]
- CTPView on CTP2000 devices do not support Y-cable redundancy on T1E1 ports. [PR/947210]
- Transparent 8 (TRANS8) encoding must be configurable from the CTPView interface. [PR/971879]

Known Issues in CTPView Release 7.0R1

This section lists the known issues in CTPView Release 7.0R1.

- PBS configured with PPP encapsulation does not function on a CTP150 device. [PR/784778]

CVEs Addressed in CTPView Release 7.0R1

The following tables list the CVEs that have been addressed in CTPView 7.0R1. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search .

Table 3: CVEs Addressed in CTPView Release 7.0R1

Kernel Patches Applied in CentOS Version 2.6.18-371.1.2.el5			
CVE-2012-3430	CVE-2012-3510	CVE-2012-2319	CVE-2012-3412
CVE-2010-3081	CVE-2008-3496	CVE-2009-1265	CVE-2009-1633
CVE-2008-5134			

Table 4: CVEs Addressed for Oracle MySQL

CVEs Addressed for Oracle MySQL 5.1.66-2.rhel5			
CVE-2013-1548	CVE-2012-3197	CVE-2012-3180	CVE-2012-3163
CVE-2012-3158	CVE-2012-3150	CVE-2012-2122	CVE-2012-1688
CVE-2012-0540	CVE-2012-1703	CVE-2012-1690	CVE-2012-5060
CVE-2012-3177	CVE-2012-3173	CVE-2012-3167	CVE-2012-3166
CVE-2012-3160	CVE-2012-2749	CVE-2012-2102	CVE-2012-1734
CVE-2012-1697	CVE-2012-1696	CVE-2012-1689	CVE-2012-0882
CVE-2012-0583	CVE-2012-0492	CVE-2012-0490	CVE-2012-0485
CVE-2012-0484	CVE-2012-0120	CVE-2012-0119	CVE-2012-0118
CVE-2012-0116	CVE-2012-0115	CVE-2012-0114	CVE-2012-0113

Table 5: CVEs Addressed in the Apache Reverse Proxy

CVEs Addressed in Apache Reverse Proxy	
CVE-2011-4317	CVE-2011-3368

Table 6: CVEs Addressed in Sudo 1.7.10p7

CVEs Addressed in SUDO 1.7.10p7			
CVE-2013-1775	CVE-2011-0010	CVE-2010-2956	CVE-2010-1646
CVE-2010-1163	CVE-2010-0426	CVE-2010-0427	CVE-2012-2337

Table 7: CVEs Addressed for PHP

CVEs Addressed for PHP 5.2.17-2			
CVE-2013-1643	CVE-2013-1635	CVE-2012-0831	CVE-2011-1398
CVE-2012-1172	CVE-2012-2329	CVE-2012-2311	CVE-2011-4566
CVE-2012-0789	CVE-2011-4885	CVE-2012-0057	CVE-2012-0781
CVE-2012-0788	CVE-2011-0708	CVE-2011-0421	CVE-2011-1153

Table 8: CVEs Addressed in SOS Package

CVEs Addressed in SOS Package
CVE-2012-2664

Table 9: RHA Advisories Addressed in the NSS and NSPR Packages

RHA Advisories Addressed in the NSS and NSPR Packages	
RHSA-2013:0214	RHSA-2013:1135

Table 10: CVEs Addressed in the CTPView FreeType Package

CVEs Addressed in the CTPView Freetype Package
CVE-2012-5669

Table 11: RHA Advisories Addressed in LibPNG Package

RHA Advisories Addressed in the LibPNG Package	
RHSA-2012:0523	CVE-2011-3048

Table 12: RHA Advisories Addressed in krb5-libs

RHA Advisories and CVEs Addressed in krb5-libs	
RHSA-2013:0942	CVE-2002-2443

Table 13: CVEs Addressed in glibc

RHA Advisories and CVEs Addressed in glibc			
RHSA-2012:0126	RHBA-2013:0885		
CVE-2009-5064	CVE-2009-5029	CVE-2010-0830	CVE-2011-1089
CVE-2011-4609			

Table 14: CVEs Addressed in PAM

CVEs Addressed in pam-0.99.6.2-12.el5			
CVE-2010-3853	CVE-2010-4707	CVE-2010-3316	CVE-2010-3435

Table 15: CVEs Addressed in libxml

CVEs Addressed in libxml			
CVE-2011-1944	CVE-2011-3919	CVE-2011-0216	CVE-2010-4008
CVE-2011-3905	CVE-2011-2834	CVE-2009-2414	CVE-2009-2416
CVE-2014-3470	CVE-2014-0224	CVE-2014-0221	CVE-2014-0195
CVE-2010-5298	CVE-2014-0076	CVE-2013-6450	CVE-2013-0169
CVE-2013-0166	CVE-2011-1473	CVE-2012-2333	

Table 16: CVEs Addressed in Mozilla NSS Library

CVEs Addressed in Mozilla NSS Library
CVE-2014-1568

Table 17: Critical or Important CVEs Included in BASH Version 3.2.33

Critical or Important CVEs Included in BASH Version 3.2.33	
CVE-2014-6271	CVE-2014-7169

CTP Documentation and Release Notes

For a list of related CTP documentation, see http://www.juniper.net/techpubs/en_US/release-independent/ctp/information-products/pathway-pages/index.html.

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 http://www.juniper.net/techpubs/.

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 postsales 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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://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.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html .

Revision History

September 2014—Revision 1, CTPView Release 7.0R1