Juniper Networks® CTPView Server Software Release 7.1R1_JITC Release Notes

Release 7.1R1_JITC
April 2015
Revision 1

These release notes accompany Release 7.1R1_JITC of the CTPView Server Software. They contain upgrade information and describe the enhancements to the software. The CTPView Release 7.1R1_JITC software is compatible with Juniper Networks CTP Series platforms running CTPOS version 7.1 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/ctp7.1/information-products/pathway-pages/ctp-series/index.html. We are publishing only the Release Notes of CTPOS and CTPView, and the Security Deployment Guides of CTPOS and CTPView for 7.1R1_JITC. These documents accurately and completely describe the enhancements and behavior changes introduced in this release. We recommend that you read these 7.1R1 documents in conjunction with the other manuals that were updated and published for 7.0R1. For easy reference, we have published the 7.0R1 manuals to the CTPOS and CTPView 7.1R1 index pages.

Contents

New Features

No new features have been added to CTPView Release 7.1R1_JITC.

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_7.1R1_JITC_150430.tgz** [software updates]
- **ctpview_complete_centos_7.1R1_JITC_150430.tgz** [software and CentOS OS updates]
- ctpview_complete_fc9_7.1R1_JITC_150430.tgz [Software and Fedora 9 OS Updates]
- ctpview_complete_fc4_7.1R1_JITC_150430.tgz [Software and Fedora 4 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 1 on page 3 to determine the correct file to use.

Table 1: 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 7.0R1 or earlier 7.1R1_JITC or earlier	**ctpview_complete_centos_7.1R1_JITC_150430.tgz**	Yes

Upgrading the CTPView Software

These sections describe how to upgrade CTPView Server Software to Release 7.1R1_JITC.

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 7.1R1_JITC

The following issues have been resolved in CTPView Release 7.1R1_JITC:

- JITC Certification for CTPView 7.1R1. [PR/1029358]
- JITC: Need Support For SRG-APP-000170-NDM-000329 in CTPView [PR/106874].
- JITC : Need support for rule SRG-APP-000001-NDM-000200 of NDM STIG [PR/1073126]

- JITC: Web Apache Rules (WA000-WWA064, WA000-WWA066, WA00500, WA00505, WA00510, WA00520, WA00525, WA00540, WA00545, WA00515 and WG360) are failed during JITC Testing [PR/1043953]
- JITC : Unix STIG rules (GEN003660 and GEN007960) are failed during JITC testing [PR/1047561]
- JITC : Unix STIG rules (GEN000450 and GEN000454) are failed during JITC testing [PR/1049038]
- JITC : Unix STIG rules (GEN005515, GEN005519, GEN005520, GEN005524,GEN005525, GEN005526 and GEN005533) are failed during JITC testing [PR/1050254]
- JITC : Unix STIG rules (GEN002719, GEN002750, GEN002751, GEN002752, GEN002800 and GEN002825) are failed during JITC testing. [PR/1050265]
- Need analysis of CVEs for CTPview and CTP susceptibility [PR/ 1052156]
- JITC : Unix STIG rules GEN003500 is failed during JITC testing [PR/ 1053882]
- JITC : Unix STIG rules GEN000590 and GEN000595 are failed during JITC testing [PR/ 1055529]
- JITC : Unix STIG rules (GEN001780, GEN002753, GEN002870 and GEN007850) are failed during JITC testing. [PR/ 1055541]
- CTPView upgrade from 4.6R1 to 7.0R1 failed [PR/ 1055729]
- JITC : Unix STIG rule GEN000588 is failed during JITC testing. [PR/ 1056694]
- Report of Vulnerabilities affecting CTPView software. [PR/ 1056715]
- JITC : Need support for Unix STIG rule GEN005495. Need to have a FIPS based OPENSSH. [PR/ 1057141]
- JITC : Unix STIG rules (GEN000251, GEN000750 and GEN003060) are failed during JITC testing. [PR/1041703]
- JITC : Unix STIG rules (GEN001720, GEN001740, GEN001820, GEN003780 and GEN005320) are failed during JITC testing. [PR /1041677]
- JITC : Unix STIG rules (GEN003600, GEN003603, GEN003609, GEN003610, GEN003611, GEN005610 and GEN007920) are failed during JITC testing. [PR/1046671]
- JITC : Unix STIG rules (GEN005506, GEN005510, GEN005511, GEN005512 and GEN005521) are failed during JITC testing. [PR/1043918]
- JITC : Unix STIG rules (GEN005536, GEN005538 and GEN005539) are failed during JITC testing. [PR/1045659]
- JITC : Unix STIG rules GEN007940 is failed during JITC testing. [PR/1050302]
- JITC : Unix STIG rules GEN000590 and GEN000595 are failed during JITC testing. [PR/1055529]
- You can enter incorrect IP addresses for NTP client and peer fields on CTPView admin page. [PR/1079115]
- Retina Scanner shows vulnerability in libgcc package in CTPView. [PR/1081226]

- Subgraph Vega shows multiple CAT I SQL Injection and Integer Overflow Vulnerabilities. [PR/1080681]
- Subgraph Vega shows multiple CAT I Cross Site Scripting Vulnerabilities. [PR/1080683]
- Kernel security update vulnerability found in Retina scan. [PR/1083557]

Known Issues in CTPView Release 7.1R1_JITC

This section lists the known issues in CTPView Release 7.1R1_JITC.

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

CVEs Addressed in CTPView Release 7.1R1_JITC

The following tables list the CVEs that have been addressed in CTPView 7.1R1_JITC. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search .

Table 2: CVEs Addressed in OpenSSL

CVEs Addressed in OpenSSL			
CVE-2015-0204 [PR/1068919]	CVE-2015-0286 [PR/1072934]	CVE-2015-0287 [PR/1072934]	CVE-2015-0289 [PR/1072934]
CVE-2015-0292 [PR/1072934]	CVE-2015-0293 [PR/1072934]	CVE-2015-0209 [PR/1072934]	CVE-2015-0288 [PR/1072934]

Table 3: CVEs Addressed in glibc

CVEs Addressed in glibc
CVE-2015-0235 [PR/1060060]

Table 4: CVEs Addressed in the Bash Package

CVEs Addressed in the Bash Package	
CVE-2014-7186 [PR/1032804]	CVE-2014-7187 [PR/1032804]

Table 5: CVEs Addressed in the Apache Package

CVEs Addressed in the Apache Package
CVE-2014-0231 [PR/1081228]

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

April 2015—Revision 1, CTPView Release 7.1R1_JITC