CTPView Management System, version 7.1R3 Software Release Notes

Release 7.1R3
23rd Sep 2016

These release notes accompany Release 7.1R3 of the CTPView Management System software. They describe the defects fixes as well as known issues with the software. CTPView Management System software runs on all CTPView appliances. This release provides management services for CTP systems running CTPOS 7.1 and below.

New Features and Enhancements:

- None.

Issues Fixed in this release:

- [PR 1144300] Multiple vulnerabilities announced by ntp.org low-medium vulnerabilities (13) Boston University (1) 14 total.
- [PR 1144746] Turn the Crank Upgrade to OpenSSL 0.9.8zh/1.0.0t/1.0.1q/1.0.2e - OpenSSL Security Advisory [03 Dec 2015].
- [PR 1157827] After upgrade, OS security level changes to high from very-low.
- [PR 1165849] CTPView Turn The Crank Upgrade to OpenSSL 1.0.1s/1.0.2g - OpenSSL Security Advisory [01 Mar 2016].
- [PR 1183185] CTPView- NTP - April 26, 2016 - Multiple low-medium vulnerabilities announced by ntp.org; some vulnerabilities announced with mitigation methods only, including previously mentioned vulnerabilities. Additionally, a previous CVE introduced a bug in NTP, and was fixed.
- [PR 1199020] Security Vulnerabilities Found during security audit performed against CTPView server running version 7.2R1.
- [PR 1201533] CTPView - httpoxy - A CGI application vulnerability for PHP, Go, Python and others.
- [PR 1203132] Security Vulnerability in glibc CVE-2013-7424.
- [PR 1205879] Retina reported NTP Vulnerability.

Known Issues:

- None.

Notes:

Security Deployment Guide
The guide is available for download at
http://www.juniper.net/techpubs/en_US/ctp7.1/information-products/pathway-pages/ctp-series/index.html

Required Files:

The full suite of security enhancements is available only when the CTPView software is installed on servers running the CentOS 5.11 Operating System. 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_7.1R3_160920.tgz [Software Updates]
- ctpview_complete_centos_7.1R3_160920.tgz [Software and CentOS OS Updates]

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

CTPView Server OS	Installed CTPView Release	File for Upgrade	Server Reboots During Upgrade ?
Cent OS 5.11	4.5R2 or earlier 4.6R1 or earlier 7.0R4 or earlier 7.1R2 or earlier	ctpview_complete_centos_7.1R3_160920.tgz	Yes

Installing Software:

On systems running 3.4R2-p1 or 3.4R3 or later:

1. Copy the File for Upgrade to the /tmp directory on the server.
2. Log into server shell.
    a. On CentOS systems as a System Administrator
3. Run the upgrade script: ***upgrade***

Note: When upgrading CentOS 5.11 systems running a release earlier than 4.1R1 you will be prompted to enter the MySQL Administrator's password. This is necessary in order to upgrade the database structures. If you fail to enter the correct password the upgrade process will continue and the server will remain usable. However, to properly complete the upgrade process you will need to manually initiate the database structure upgrade script from the cli menu. The path to this function is menu > MySQL Functions > Upgrade Database Structures.

On systems running 3.4R2 or earlier and requiring a ctpview_complete file:

1. Copy the Upgrade File to the /tmp directory on the server.
2. Log into server shell. Switch to the **root** user after log in.
3. Unpack the ctpview_complete file. For example,
   tar –xzvf ctpview_complete_centos_7.1R3_ 160920.tgz
4. Run the upgrade script: ***upgrade***

On systems running 3.4R2 or earlier and requiring the web_update file:

1. Copy the Upgrade File to the /tmp directory on the server.
2. Log into server shell. Switch to the **root** user after log in.
3. Run the upgrade script: ***upgrade***

Note: - Disable all the ports/bundles of the CTP box before initiating the CTPOS upgrade process using CTP complete package.