CTPView Management System, version 7.1R4 Software Release Notes

Release 7.1R4
21st Aug 2017

These release notes accompany Release 7.1R4 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 1222844] CTPView Secondary syncing results in server losing connectivity to all of the CTP nodes.
- [PR 1226969] CTPView - CVE-2016-5195 - "dirty COW" Linux Kernel Local Privilege Escalation
- [PR 1234181] November 2016 ntp-4.2.8p9 NTP Security Vulnerability Announcement
- [PR 1240574] Cannot add a second eth to a ESXi VM CT View
- [PR 1249154] When doing a manual sync from a primary to secondary ctpview server, partial transfers are seen
- [PR 1249814] CTPView: OpenSSL 1.0.2k, 1.1.0d - OpenSSL Security Advisory [26 Jan 2017]
- [PR 1265415] NetMon stops polling CTP hosts
- [PR 1283207] CTPView secondary sync server cannot reach CTPs after a sync event
- [PR 1283224] mysqld.log files can grow to be huge > 1Gb
- [PR 1283874] Cannot https log into ctpview using IPV6
- [PR 1284155] CVE-2017-6074 fix in CTPOS, A use-after-free flaw was found in the way the Linux kernel's Datagram Congestion Control Protocol (DCCP) implementation freed SKB (socket buffer) resources for a DCCP_PKT_REQUEST packet when the IPV6_RECVPKTINFO option is set on the socket. A local, unprivileged user could use this flaw to alter the
- [PR 1296274] CTPView Server supports SSL 64-bit block size Cipher suites
- [PR 1296278] CTPView web server is affected by an information disclosure vulnerability.

Known Issues:

- None.

Notes:

Customers running CTP View servers with older browsers like NCSA Mosaic can no longer connect to the CTPView server. This is for the reason that to address SIRT PR 1296274, SSLCipherSuite string has been changed.

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_7.1R4_170817.tgz [Software Updates]
- ctpview_complete_centos_7.1R4_170817.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 7.1R3 or earlier	ctpview_complete_centos_7.1R4_170817.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_7.1R4_170817.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***