Method of Procedure to Apply Red Hat Enterprise Linux 6.1/6.7 Security Vulnerability Patch on RMS

First Published: February 15, 2016

Table of Contents

Scope of MOP

This document describes the procedure to apply the Red Hat Enterprise Linux 6.1/6.7 security vulnerability patch on all the RMS Nodes.

Prerequisites

- AIO/Distributed RMS Setup (RMS, Release 5.1) should be deployed and all the processes are up and running.
- Verify that the DPE is in ready state from BAC UI > Servers > DPEs, click on the DPE and check the state is Ready.
- RMS should be on Red Hat Enterprise Linux 6.1 or 6.7.
- If the RMS setup is a distributed redundant deployment then inter-VM communication should be configured.
- All the RMS Nodes should be able to access the public Red Hat server by adding additional rule in IPtables or by stopping the IPtables.
- Red Hat server account should be available.
- The openssl, python-rhsm, python-dateutil and subscription-manager rpms should be equal to or greater than the below versions

Enter:	`# rpm -qa|egrep "openssl|python-rhsm|python-dateutil|subscription"`

Output:	`[rms-aio-central] ~ $ rpm -qa|egrep "openssl|python-rhsm|python-dateutil|subscription"`
	`subscription-manager-1.14.10-1.el6.x86_64`
	`python-rhsm-1.14.3-1.el6.x86_64`
	`openssl-1.0.1e-30.el6_6.11.i686`
	`openssl-1.0.1e-30.el6_6.11.x86_64`
	`python-dateutil-1.4.1-6.el6.noarch`
	`[rms-aio-central] ~ $`

Assumptions

It is assumed that the user has firm knowledge and familiarity with using LINUX from the shell command line. For example, the user should know about the following (this is not a comprehensive list):

- How to login to a command line session (typically as root)
- How to SSH to server using putty or terminal.
- Basic IP networking (IP addresses, network masks, etc.)
- VMWare vSphere access
- MOP assumes VMware is with ESXi5.5
- IPs of the central node, serving nodes, upload nodes and DNS entries are available and user can login to RMS nodes and execute commands in super user mode.

- Assuming AIO/Distributed RMS deployment mode.
- Assuming the data store has sufficient free space to clone the nodes.
- Assuming that the user has access to the Red Hat Account.
- Lab admin provide access of RMS nodes to Pubic RHEL servers prior to MOP execution and disables it after MOP execution if needed.

Disable RMS Northbound and Southbound Traffic

Disabling RMS Northbound Traffic

To disable the northbound traffic, stop provisioning from the IT interface.

Disabling RMS Southbound Traffic

Procedure

1. Log in to the Central Node VM and ping the eth1 IP (refer, ifconfig) of the Serving node and Upload node (from the central node) and ensure that the IP is reachable.
2. Log in to the vSphere Web Client and locate the Serving and Upload node VM or vApp
3. Right-click on the Serving and Upload node VM and click **Edit Settings.**
4. Identify the corresponding network adapter or VLAN of the Southbound interface (refer the descriptor file used for installing the RMS system to identify the VLAN of the Serving and Upload node Southbound interface, that is, the property value of 'net:Serving-Node Network 2').
5. Uncheck the **Connected** checkbox of the network adapter or VLAN of the Serving and Upload node Southbound interface.
6. Click **Ok**.
7. To verify that the interface is down, ping the eth1 IP (refer, ifconfig) of the Serving and Upload node (from the central node) and ensure that the IP is not reachable.
8. Repeat the steps on the redundant Serving and Upload node in case of redundant setup.

Pre Maintenance

Clone the System

Backup the System using vApp Cloning

Procedure

1. Login to the VM to be cloned and execute the following command as a root user:

Enter:	`# mv /etc/udev/rules.d/70-persistent-net.rules /root`
Output:	`The system responds with the command prompt`

2. Login to the vSphere web client and locate the vApp of the VM to be cloned, right click on the vApp and click **Power Off.**

Note: Steps 3 to 6 should be performed only on the Upload Node only if it has additional hard disks configured.

3. After the vApp is successfully powered off, right click on the **Virtual Machine** and click **Edit Settings.**
4. Click on the additionally configured hard disk (other than the default hard disk – Hard Disk 1). For Example, Hard Disk 2, Hard Disk 3, Hard Disk 4.
5. Record the Disk File from the drop-down.

Note: Record can be a making a note of the disk file to a text file on the local machine to add it back later.

6. Close the drop-down and remove (to remove click on the 'X' symbol against each additionally added hard disk) the additional hard disks. Example, Hard Disk 2, Hard Disk 3, Hard Disk 4, so on and click on **OK.**

Note: Upon removing the additional hard disks do not check the checkbox because that would delete the files from the data store which cannot be recovered.

7. Right click on the vApp and select **All vCenter Actions** and click **Clone.** The New vApp wizard is displayed.
8. In the **1a Select a creation type** tab, select **Clone an existing vApp** and click on **Next.**
9. In **2a Select destination** tab, select the host in which the clone has to be taken and click on **Next**.
10. In **2b Select a name and location** tab, provide a unique vApp name for the clone and select the target folder/datacenter and click on **Next**.
11. In **2c Select storage** tab, select where to store the files of the vApp and click on **Next**.
12. Click on **Next** in **2d Map networks, 2e vApp properties, 2f Resource allocation** tabs.
13. In the **3 Ready to complete**, click on **Finish**.
14. The status of the clone will be seen in the Recent Tasks section on the right top corner of the vSphere web client.

Note: Follow the above procedure on all the RMS Nodes.

Maintenance Activity

Verify the Red Hat Enterprise Linux Version on RMS Nodes

1. Login to the RMS nodes (Central, Serving, upload) as a root user and verify that the Red Hat Enterprise Linux version is 6.1 or 6.7

Enter:	# **cat /etc/redhat-release**
Output:	Red Hat Enterprise Linux Server release 6.1 or 6.7 (Santiago)

Configuring the DNS IP

2. Ensure that the '/etc/resolv.conf' file has the correct DNS server IP to resolve the red hat subscription manager.

Enter:	# **cat /etc/resolv.conf**
Output:	nameserver <DNS IP>

If the configured DNS IP has to be changed then as a root user execute the below command to configure the DNS server IP

Enter:	**# echo "nameserver <DNS IP1>" >> /etc/resolv.conf** **# echo "nameserver <DNS IP2>" >> /etc/resolv.conf** Note: Replace <DNS IP1> or <DNS IP2> with correct DNS IP
Output:	The system responds with the command prompt

Backup the DNS configuration

As a 'root' user backup of the /etc/resolv.conf file with valid DNS IP.

Enter:	**# cp /etc/resolv.conf /home/admin1**
Output:	The system prompts with command prompt and the file

Verify Red Hat Subscription Manager Configuration

3. Verify that Red Hat Subscription Manager configuration is present on the system.

Enter:	**cat /etc/rhsm/rhsm.conf**

Output:	[rms-aio-central] ~ # cat /etc/rhsm/rhsm.conf
	# Red Hat Subscription Manager Configuration File:
	
	# Unified Entitlement Platform Configuration
	[server]
	# Server hostname:
	hostname = subscription.rhn.redhat.com
	
	# Server prefix:
	prefix = /subscription
	
	# Server port:
	port = 443
	
	# Set to 1 to disable certificate validation:
	insecure = 0
	
	# Set the depth of certs which should be checked
	# when validating a certificate
	ssl_verify_depth = 3
	
	# Server CA certificate location:
	ca_cert_dir = /etc/rhsm/ca/
	
	# an http proxy server to use
	proxy_hostname =
	
	# port for http proxy server
	proxy_port =
	
	# user name for authenticating to an http proxy, if needed
	proxy_user =
	
	# password for basic http proxy auth, if needed
	proxy_password =
	
	[rhsm]
	# Content base URL:
	baseurl= https://cdn.redhat.com
	
	# Default CA cert to use when generating yum repo configs:
	repo_ca_cert = %(ca_cert_dir)sredhat-uep.pem
	
	# Where the certificates should be stored
	productCertDir = /etc/pki/product
	entitlementCertDir = /etc/pki/entitlement
	consumerCertDir = /etc/pki/consumer
	
	[rhsmcertd]
	# Frequency of certificate refresh (in minutes):
	certFrequency = 240
	
	[rms-aio-central] ~ #

If there are any manual changes done to "/etc/rhsm/rhsm.conf" file (eg., proxy settings are updated) then restart the rhsmcertd service using the below command to make the changes effective.

Enter:	**# service rhsmcertd restart**

Output:	[rms-aio-central] ~ # service rhsmcertd restart Stopping rhsmcertd [OK] Starting rhsmcertd 240 [OK] [rms-aio-central] ~ #

Locale Settings

4. Verify the locale settings to identify if the user language configured

Enter:	**# locale**

Output:	**Note: Below is just a sample and may vary from system to system.**
	
	[rms-aio-central] ~ # locale
	LANG=en_US.UTF-8
	LC_CTYPE="en_US.UTF-8"
	LC_NUMERIC="en_US.UTF-8"
	LC_TIME="en_US.UTF-8"
	LC_COLLATE="en_US.UTF-8"
	LC_MONETARY="en_US.UTF-8"
	LC_MESSAGES="en_US.UTF-8"
	LC_PAPER="en_US.UTF-8"
	LC_NAME="en_US.UTF-8"
	LC_ADDRESS="en_US.UTF-8"
	LC_TELEPHONE="en_US.UTF-8"
	LC_MEASUREMENT="en_US.UTF-8"
	LC_IDENTIFICATION="en_US.UTF-8"
	LC_ALL=
	[rms-aio-central] ~ #

If the locale is not with the expected value then set the locale as show in the example below.

Enter:	# **LANG="en_US.UTF-8"** **Note: This is just an example for English – United States and content inside quotes can to be changed as required.**
Output:	The system responds with the command prompt

Register RMS Node to Red Hat Service

5. Register the Virtual Machine to the Red Hat service by providing registered user details (username, password) when prompted.

Enter:	# **subscription-manager register**
Output:	[rms-distr-central] ~ # subscription-manager register Username: rhusername Password: ******* The system has been registered with ID: 542ac5c5-4e47-46dc-a86f-af662489b74f [rms-distr-central] ~ #

Note: If the above registration command fails with "sslv3 alert handshake failure" then the rpms are not updated as mentioned in the pre-requisites, hence update the rpms and repeat "Register RMS Node to Red Hat Service"

Download certificate file for the System

6. Login to the Red Hat Account and navigate to SUBSCRIPTIONS > Red Hat Subscription Management > Subscriber Inventory > Systems, select the system (appropriate hostname of the VirtualMachine) and then click on **Run Auto-Attach**, verify that there is an option to download the **Entitlement Certificate** from **Attached Subscription** tab, Click on download and copy the .pem file to the system (system whose .pem file was downloaded).

Import the certificate file into the system

7. Import the previously downloaded certificate (.pem) file onto the system.

Enter:	**# subscription-manager import --certificate=<.pem file name with extension>**
Output:	[rms-distr-central] ~ # subscription-manager import --certificate=8a85f9 8151352075015137df54a41aca.pem Successfully imported certificate 8a85f98151352075015137df54a41aca.pem [rms-distr-central] ~ #

Verification of the RMS Node Subscription

8. Verify if the RMS Node is subscribed to the Red Hat

Enter:	**# subscription-manager list**
Output:	[rms-distr-central] ~ # subscription-manager list +---+ Installed Product Status +---+ Product Name: Red Hat Enterprise Linux 6 Server Product ID: 69 Version: 6.7 Arch: x86_64 Status: **Subscribed** Starts: 11/24/2015 Ends: 11/24/2015 [rms-distr-central] ~ #

Disabling the pre-existing local repository

9. Disable any local repository present in "/etc/yum.repos.d/".

Enter:	**# /etc/yum.repos.d/system.repo** **Note: Here system.repo is a sample file**
Output:	[rms-distr-central] /etc/yum.repos.d # cat system.repo [systemrepo] name=systemrepo baseurl=file:///rhel67/ gpgcheck=0 **enabled=0** [rms-distr-central] /etc/yum.repos.d #

Install the Red Hat Enterprise Linux 6.1/6.7 security patch

10. Clean any existing yum configuration from the system

Enter:	# **yum clean all**
Output:	[rms-distr-central] ~ # yum clean all Loaded plugins: product-id, security, subscription-manager Cleaning repos: rhel-6-server-rpms Cleaning up Everything [rms-distr-central] ~ #

11. Apply the command to install the security rpm

Enter:	**# yum install yum-security** **Note: Upon executing the above command provide response [y] for prompts asking permission**

Output:

```
[rms-distr-central] ~ # yum install yum-security
Loaded plugins: product-id, subscription-manager
rhel-6-server-rpms
| 3.7 kB     00:00
rhel-6-server-rpms/primary_db
|  36 MB     00:36
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package yum-plugin-security.noarch 0:1.1.30-30.el6 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
== Package                                                  Arch
Version                                          Repository
Size
================================================================================
==Installing:
 yum-plugin-security                                   noarch
1.1.30-30.el6                                    rhel-6-server-rpms
41 k

Transaction Summary
================================================================================
Install       1 Package(s)

Total download size: 41 k
Installed size: 79 k
Is this ok [y/N]: y
Downloading Packages:
yum-plugin-security-1.1.30-30.el6.noarch.rpm
|  41 kB     00:00
warning: rpmts_HdrFromFdno: Header V3 RSA/SHA256 Signature, key ID fd431d51:
NOKEY
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Importing GPG key 0xFD431D51:
 Userid : Red Hat, Inc. (release key 2) <security@redhat.com>
 Package: redhat-release-server-6Server-6.7.0.3.el6.x86_64 (@anaconda-
RedHatEnterpriseLinux-201507020259.x86_64/6.7)
 From   : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Is this ok [y/N]: y
Importing GPG key 0x2FA658E0:
 Userid : Red Hat, Inc. (auxiliary key) <security@redhat.com>
 Package: redhat-release-server-6Server-6.7.0.3.el6.x86_64 (@anaconda-
RedHatEnterpriseLinux-201507020259.x86_64/6.7)
 From   : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
Warning: RPMDB altered outside of yum.
** Found 3 pre-existing rpmdb problem(s), 'yum check' output follows:
CSCObac-rdu-3.10.1-201509210944_95.i386 has missing requires of libdb-5.1.so
CSCObac-rdu-3.10.1-201509210944_95.i386 has missing requires of libjvm.so
CSCObac-rdu-3.10.1-201509210944_95.i386 has missing requires of
libjvm.so(SUNWprivate_1.1)
 Installing  : yum-plugin-security-1.1.30-30.el6.noarch
1/1
rhel-6-server-rpms/productid
| 1.7 kB     00:00
  Verifying  : yum-plugin-security-1.1.30-30.el6.noarch
1/1

Installed:
  yum-plugin-security.noarch 0:1.1.30-30.el6

Complete!  Installing : yum-plugin-security-1.1.30-30.el6.noarch
1/1
```

12. Update the minimal security updates

Enter:	**# yum update-minimal –security** **Note: Upon executing the above command provide response [y] for prompts asking permission**
Output:	yum update-minimal --security Loaded plugins: product-id, security, subscription-manager rhel-6-server-rpms/updateinfo | 2.9 MB 00:02 Resolving Dependencies --> Running transaction check ---> Package bind-libs.x86_64 32:9.8.2-0.37.rc1.el6 will be updated .. .. Transaction Summary ========== ========== ========== Install 1 Package(s) Upgrade 37 Package(s) Total download size: 73 M **Is this ok [y/N]: y** Downloading Packages: .. .. Installed: kernel.x86_64 0:2.6.32-573.12.1.el6 Updated: .. .. Complete!

Unregister RMS Node from Red Hat Service

13. After the rpms are installed and updated unregister the RMS Node from Red Hat Service by providing the registered user details (username, password) when prompted

Enter:	# subscription-manager unregister
Output:	[rms-distr-central] / # subscription-manager unregister System has been unregistered. [rms-distr-central] / #

Central Node Updates

Note: Skip the below updates on the serving and upload nodes

14. After the successful rpm updates perform the below steps on the CENTRAL NODE

    a. As a root user revert the postgres port setting.

        i. If RMS version is 4.1, then do the setting as below

Enter:	# **sed -i 's/PGPORT=5432/PGPORT=5435/' /etc/rc.d/init.d/postgresql**
Output:	The system responds with the command prompt

ii. If RMS version is 5.1 or 5.1MR, then do the setting as below

Enter:	# **sed -i 's/PGPORT=5432/PGPORT=5439/' /etc/rc.d/init.d/postgresql**
Output:	The system responds with the command prompt

b. As a root user stop the 'NetworkManager'.

Enter:	**# service NetworkManager stop** **# chkconfig NetworkManager off**
Output:	The system responds with the command prompt

c. Ensure that the '/etc/resolv.conf' file has the DNS server IP.

Enter:	# **cat /etc/resolv.conf**
Output:	nameserver <DNS IP>

If the '/etc/resolv.conf' file doesn't have the DNS server then as a 'root' user copy back the backed up file.

Enter:	# **cp /home/admin1/resolv.conf /etc/**
Output:	[rms-distr-central] / # cp /home/admin1/resolv.conf /etc/ cp: overwrite `/etc/resolv.conf'? **y** [rms-distr-central] / #

Reboot the System

15. Reboot the system for all the changes to reflect

Enter:	# **reboot**
Output:	Broadcast message from admin1@rms-aio-central (/dev/pts/0) at 12:09 ... The system is going down for reboot NOW!

Start VMWare Tools Application

16. Start the VMWare Tools application on all the RMS Nodes and verify if its running

Enter:	# **/usr/bin/vmware-config-tools.pl -d**

Output:	The system responds with the command prompt Login to the vSphere Web Client and locate the **Virtual Machine** and on the **Summary** tab verify that the **VMware Tools** status is **Running**.

Maintenance Verification

17. Verify that all the RMS Nodes (Central, Serving, Upload and redundant serving, upload node if any) are up and running
18. Verify that the User Interfaces of RMS are accessible.
19. Ensure DPE is in Ready state after the maintenance activity from BAC UI > Servers > DPEs, click on the DPE and check the state is Ready.

Enable RMS Southbound and Northbound Traffic

Enabling RMS Southbound Traffic

Procedure

1. Log in to the vSphere Web Client and locate the Serving and Upload node VM or vApp.
2. Right-click on the Serving and Upload node VM and click **Edit Settings**.
3. Identify the corresponding network adapter or VLAN of the Southbound interface (refer Step4 of Disabling RMS Southbound Traffic)
4. Check the Connected checkbox of the network adapter or VLAN of the Serving and Upload node southbound interface.
5. Click **Ok.**
6. To verify that the interface is up, ping the eth1 IP (refer, ifconfig) of the Serving and Upload node (from the Central Node) and ensure that the IP is reachable.
7. Repeat the steps on the redundant Serving and Upload node in case of redundant setup.

Enabling RMS Northbound Traffic

To enable the northbound traffic, start the provisioning from IT interface.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)