Product Support Notice

© 2020 Avaya Inc. All Rights Reserved.

PSN #	PSN005673u				
Original publication date: 1-Sep-2020. This is Issue #3, published date: 11-Sep-2020.		Severity/risk level	Low	Urgency	When convenient

Name of problem

CMS Linux RPM update

Products affected

CMS 19.1.0.1

Problem description

This PSN provides information about a new 'Linux RPM Update' procedure available for CMS.

The purpose of the 'Linux RPM Update' procedure is to make RedHat Linux RPM updates available to customers in between CMS Service Packs.

The naming convention for the 'Linux RPM Update' downloadable file is:

rpm_update_R<*x.y.z*>L<*load-number*><*version-number*>.bin

As an example, the first 'Linux RPM Update' is rpm_update_*R19.1.0.1*L*fb.i.1*.bin

Where R19.1.0.1: is the version of CMS to which the RPM Updates apply

fb.i: is the specific CMS load number

.1: is the version of the RPM update .bin file

The binary file will only install on the version and load number indicated in the name of the file. Thus the currently available RPM Update only applies to CMS 19.1.0.1

If users attempt to install the Linux RPM Updates on other versions of CMS, the install will fail with an error message informing the user that the version of CMS is not compatible with the Linux RPM Update.

It is expected that customers upgrade to CMS 19.1.0.1, then install the Linux RPM Update, if desired. The Linux RPM Update is not required, and is optional.

The binary file is available now for download on support.avaya.com under 'Downloads' for CMS 19.1.

The Linux RPM Update will update all RPMs on CMS 19.1.0.1 to the version of the RPMs available at the time the update is deployed to customers.

The downloadable file and install procedure is very similar to a standard CMS patch deployment. See the 'Patch Install' section of this PSN for details.

Resolution

n/a

Workaround or alternative remediation

n/a

Remarks

This PSN will be updated as new CMS 19.1 Linux RPM Updates become available

RPM Update file name	Version Number	Notes	Date
rpm_update_R19.1.0.1Lfb.i.1.bin	1	First CMS 19.1 Linux RPM Update	August, 28, 2020

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the RPM Updates

n/a

Download

The Linux RPM Update file is available on support.avaya.com under the 'Downloads' tab for CMS 19.1

Patch install instructions

Service-interrupting?

a

The Linux RPM Update procedure is very similar to a patch install for CMS.

The installation of Linux RPM updates is service effecting, the CMS will be rebooted. Further, CMS web must be stopped prior to installing the rpm updates, and the OA forwarder must be stopped if it is installed.

Installation Procedure:

1. Download rpm_update_R19.1.0.1Lfb.i.1.bin to / on the CMS server.
2. Check the md5 sum of the downloaded file. It should be
   e2a46fa591da80e683e0f885cd1fb677
3. Go to the / directory where you placed the .bin file
   a. Prompt> cd /
4. Get the checksum for the downloaded .bin file
   a. Prompt> md5sum rpm_update_R19.1.0.1Lfb.i.1.bin
5. Compare the output of this command to the above number, they should match
   a. If the numbers do not match, there was a problem with the download, try downloading again
6. Stop the CMS Web process
   a. Prompt> cmsweb stop
7. Stop the OA forwarder if installed
   a. Prompt> pa stop all
8. Stop CMS
   a. Prompt> cmssvc->4) run_cms->2) Turn off both CMS and IDS
9. Chmod on the downloaded file to make it executable
   a. Prompt> chmod 744 rpm_update_R19.1.0.1Lfb.i.1.bin
10. Execute: ./rpm_update_R19.1.0.1Lfb.i.1.bin
    Answer 'y' to the following prompt: **Note the system will automatically be rebooted**
    R19.1.0.1Lfb.i RHEL rpms will be updated with RPM Version: 1, then the system will be rebooted. Do you want to continue (y or n)?
11. After reboot, execute: /storage/cms_dvd/security/cms_sec
12. Start CMS
    a. Prompt> cmssvc->4) Run CMS->1) Turn on CMS
13. Start the CMS Web process
    a. Prompt> cmsweb start
14. Start the OA forwarder if installed
    a. Prompt> pa start all

Logging is in the standard rpm_update.log: /var/cms/spatches/rpm_update.log

Verification

n/a

Failure

If the Linux RPM Update fails see the rpm_update.log: /var/cms/spatches/rpm_update.log for detailed information

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.