Product Support Notice

© 2014 Avaya Inc. All Rights Reserved.

PSN #	PSN004111u				
Original publication date: 12-Jun-14. This is Issue #01, published date: 12-Jun-14.		Severity/risk level	Medium	Urgency	Optional

Name of problem CMS Supervisor Login Procedure for password resets after password expiration may hang.

Products affected

CMS Server R17 all platforms that use the Supervisor ssh connection with auto login

Problem description

In R17 CMS Supervisor ssh connection sessions , a dialog box may hang after the user supplies password reset information for expired passwords if the user is logging into CMS from a computer where the login has not been previously used. This can be corrected with a workaround procedure.

This does not occur if the user has logged into CMS from that computer prior to the password reset.

Resolution

Software changes will be added in a future CMS release.

Workaround or alternative remediation

Customers can choose one of several workarounds for this problem depending on their situation:

Workaround 1 – Avoid the issue the first time you log into CMS from a given computer.

- Login into the CMS via the CMS Supervisor ssh connection.
- Logout
- Login in again and reset the password.

Workaround 2 – Avoid the issue by using a different login connection

- Reset the expired password using the CMS webclient instead of the CMS Supervisor ssh connection.

OR

- Reset the expired password using the CMS Supervisor telnet connection instead of the CMS Supervisor ssh connection.

Workaround 3 – Recover the Hung Session

- The user can click cancel, login again, and the new password will work.

OR

- The user can wait for timeout, login again, and the new password will work.

Workaround 4 – Use the CMS Supervisor LA_25 and R17 R3 patch 1

This problem can be corrected with an r17ja.k patch 1 and CMS Supervisor LA_25 or higher. Note: both are required to resolve this issue.

Customers should contact their Avaya support organization or business partner regarding the installation of patch patch. Customers should install the latest version of CMS Supervisor, LA_25 or higher. This is available via free download from www.support.avaya.com.

Follow the instructions below to install the r17ja.k.1 patch. **Note:** Installation of this patch is service affecting. CMS should be turned off before patch installation.

For Solaris SPARC systems:

1. Download r17ja.k.1-s.tar to / on the CMS system.
2. Check the md5 sum of the downloaded file. It should be *efff69af634945216be5586d23321c7b*.
    1. *cd /*
    2. *# digest -v -a md5 r17ja.k.1-s.tar*
       md5 (r17ja.k.1-s.tar) = efff69af634945216be5586d23321c7b
3. Turn off CMS
4. Install the patch
    1. *tar xvf r17ja.k.1-s.tar*
    2. */cms/cmspatches/cmspatch_install_script*
    3. *Follow prompts to install*

5. Turn on CMS

For Solaris x86 systems:

1. Download r17ja.k.1-x.tar to / on the CMS system.
2. Check the md5 sum of the downloaded file. It should be *9d6f79f53d45ab5c921b0146b8b66c7d*.
    - *cd /*
    - *# digest -v -a md5 r17ja.k.1-x.tar*
      md5 (r17ja.k.1-x.tar) = 9d6f79f53d45ab5c921b0146b8b66c7d
3. Turn off CMS
4. Install the patch
    - *tar xvf r17ja.k.1-x.tar*
    - */cms/cmspatches/cmspatch_install_script*
    - *Follow prompts to install*
5. Turn on CMS

For Linux systems:

a) Download r17ja.k_cmsp1-l.bin to /tmp on the CMS system.
b) Check the md5 sum of the downloaded file. It should be cad0846e9773733f264151c1e41d71c5
    - *cd /*
    - *# md5sum r17ja.k_cmsp1-l.bin*
      cad0846e9773733f264151c1e41d71c5 *_cmsp1-l.bin*
c) Turn off CMS
d) Install the patch
    - *./r17ja.k_cmsp1-l.bin*
    - Follow prompts to install.
e) Turn on CMS

Remarks

n/a

Patch Notes

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

Backup before applying the patch

n/a

Download

n/a

Patch install instructions

n/a

Service-interrupting?

No

Verification

n/a

Failure

n/a

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

© 2014 Avaya Inc. All Rights Reserved.

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.

© 2014 Avaya Inc. All Rights Reserved.