



Product Support Notice

© 2020 Avaya Inc. All Rights Reserved.

PSN # PSN005699u

Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 12-Oct-2020. This is Issue #01, published date: 12-Oct-2020.

Severity/risk level

High

Urgency

Immediately

Name of problem

New OSS patch scheduled for October 12 2020

Products affected

Powered By IP Office, Powered By IP Office Contact Center, Operations Support System

Problem description

New OSS patch that requires a non-standard procedure to upgrade

Resolution

The new OSS release includes a new GPG signature which require validation. Because of the new signature, the standard OSS upgrade procedure will fail. Customer will need to follow the below instructions in order to upgrade.

Future upgrades of OSS will work with the standard procedure.

Please follow the below process to upgrade OSS to the latest version.

1. Open an SSH session to the designated OSS server.
2. Download and validate the GPG key.

- a. Enter the following command to download the key to the `/etc/pki/rpm-gpg/` directory for **yum** to find it:

```
sudo curl -o /etc/pki/rpm-gpg/RPM-GPG-KEY-avaya-oss \ http://yum.avaya.com/oss-repo/RPM-GPG-KEY-avaya-oss
```

Do not add any spaces or characters after `\` in the command.

- b. Enter the following command:

```
gpg --quiet --with-fingerprint /etc/pki/rpm-gpg/RPM-GPG-KEY-avaya-oss
```

- c. Ensure the displayed fingerprint is:

C848 3CF9 036A 082B 9CFF 1408 4A80 8D88 2296 115A

! Important:

If the displayed key signature does not match, do not proceed.

3. To view the version of OSS that is currently installed, run the following command:

```
yum list avaya-oss
```

4. Run the following command to perform the upgrade:

```
sudo yum update avaya-oss
```

5. When prompted to answer yes or no, enter **y** or **yes**.

You will receive a question from **yum** about whether to import `/etc/pki/rpm-gpg/RPMGPG-KEY-avaya-oss` and `/etc/pki/rpm-gpg/RPM-GPG-KEYCentOS-6`.

6. To ensure OSS uses the latest kernel version, reboot the operating system.

item	Additional details
Bug fix where OSS will show error refreshing license even while the license was downloaded and working properly	In some cases, after a subscription change, the OSS subscription details page will show wrong date in the “license Refresh Failed Since” parameter, and will color this parameter red in the OSS subscription details page. This will happen in spite of the fact that the license was actually downloaded correctly. The error will clear after a few days.
Several improvements with contacting Avaya backend services.	Resolve possible license deletion problem caused by communication problems with A1S. Resolve and issue where OSS may try repeatedly to request licenses from A1S in a specific scenario.
Changes in timing of requests to A1S	These changes are introduced to reduce number of overall requests from OSS and increase the success rate of the requests
Fixing script that automatically extends expiry date of self-signed certificates	When using the default self-signed certificate in OSS, this change fix a bug where it would not automatically renew after 3 years.
Extending the license request period to 7 days	This change will cause OSS to initiate license renewal 7 days before expiry instead of 3 days. This will provide more time to react in case there is a problem with the license renewal. In case of license renewal issue OSS will alert every day.

For further details, please refer to OSS release Notes
[Operations Support System 3.0.0.0 Release Notes](#)

Workaround or alternative remediation

n/a

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

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.