Product Support Notice

© 2018 Avaya Inc. All Rights Reserved.

PSN # PSN020341u

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

Original publication date: 23-Feb-2018, published date: 23-Feb-2018. Severity/risk level* Medium Urgency* Immediately

Name of problem* AS5300 R3 SP 14.2

Products affected*

Avaya Aura® Application Server 5300 (AS 5300) Release: 3.0 SP11 - SP14.1

Problem description*

This PSN covers the following areas:

1) Linux security updates
2) Tomcat security update
3) JRE quarterly security/bugfix update
4) MCP application update
5) UC Client update
6) 11xx SIP Phone update

Resolution*

This SP contains the following updates:

OS security patches for the following packages (refer to the platform release notes for full security details):

- bind, bind-libs, bind-utils
- kernel, kernel-headers, kernel-firmware (includes the available RedHat fixes for RHSA-2018 (Spectre))
- JRE (upversion to 1.8.0_162)

MCP Application update for (refer to Release Bulletin for further information):

- AS5300DEV-26516 AS5300 3.0 SP14.1: ./resync.pl is failed to restore database from Primary host to Secondary host (mismatch license)
- AS5300DEV-26520 1-13362885043 - DISA - single address or url for the xmpp users
- AS5300DEV-26519 1-13358945190 - Lackland AFB - Active SESM does not stay active Critical All Calls failing.
- AS5300DEV-26536 1-13445690315 - resetProvAdminPasswd.pl not reseting password

UC Client

- Oracle SE Logo updated on help/about windows

11xx SIP Phone:

- 1-13195294713 - Hanscom - 1100 series phones factory default does not factory default SIP DEV_CERT version number
- 1-13231772551 (Hanscom AFB,Eglin AFB) Unable to download device certificate after Factory reset

Internal connections between all network elements are now automatically configured for TLS 1.2. This internal TLS mesh is not configurable and is enabled at all times after this upgrade. The IPSec mesh is no longer needed between AS5300 servers.

If IPSec between AS5300 and Switch Expert is not required by site personnel, it is recommended to leave IPSec completely disabled. If required, One (1) IPSec connection can be setup between the AS5300 EM/AM servers and Switch Expert. The full IPSec mesh used between all servers must not be enabled or server degradation could occur. SP14.3 will contain the TLS connection to Switch Expert and will see the completion of the IPSec replacement feature.

UPGRADE NOTE: Due to a security requirement to remove all weak ciphers, there is an additional step that MUST be taken prior to upgrading to SP14.2. Refer to the Release Bulletin for details.

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

Please follow the backup guidance in the 103.1.2 AS 5300 3.0 Software Update MOP for instructions for installing the patches.

Download

All files can be found on the AS 5300 R3 SP14.2 support portal webpage.

Patch install instructions — Service-interrupting?

Yes

NOTE: Due to a security requirement to remove all weak ciphers, there is an additional step that MUST be taken prior to upgrading to SP14.2. Refer to the Release Bulletin for details.

Follow the AS 5300 R3.0 update procedures as documented in 103.1.2 AS 5300 3.0 Software Update MOP to apply all of the patches.

Verification

To verify the OS platform version after applying the platform patch:

1) Log into the SIP Core or AMS server as a user in the SSA role
2) Run the following command:

   mcpRelease.pl

Example output:

[sysadm@server4879-vm01 ~]$ mcpRelease.pl

*** MCP Platform Release ***

System Type: mcp_core_linux_ple2
Release Level: **15.0.70** (via patching)
Hardware Env: VMware Virtual Machine

To verify the MCP version after applying the MCP Patch:

Verify that the title of the EM Console window to ensure the version listed matches the SP14.2 MCP Patch version.

Verify Tomcat upgrade as follows:

1) Log into the EM server as a user in the SSA role
2) Run the following command:

   showversion

Example output:

© 2017 Avaya Inc. All Rights Reserved.

[sysadm@server4879-vm01 ~]$ showversion

Tomcat Version: **8.0.48**

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.