**Name of problem**
AS5300 R3 SP 15.3

**Products affected**
Avaya Aura® Application Server 5300 (AS 5300) Release: 3.0 SP11 - SP15.2

**Problem description**
This PSN covers the following areas:
1) Linux security updates
2) Database security update
3) Tomcat security update
4) MCP application update

**Resolution**
This service pack contains the following updates:

**Linux security patches for the following packages (refer to the platform release notes for full security details):**
- Java
- bind
- dbus
- sudo
- kernel
- openssl
- polkit
- python
- vim

**Database update:**
- up-versioned to 9.6.15-8

**Tomcat update:**
- up-versioned to 9.0.27

**MCP Application update:**
- 1-13705970327 - AS5300 - Call to Emergency DN failing with blocked precedence
- 1-14649058900 long distance trunks calling out the MG3k LE with sequential order will not overflow to the second T1

**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 AS 5300 R3.0 SP15.3 files can be found on the AS 5300 R3 SP15.3 support portal webpage.

<table>
<thead>
<tr>
<th>Patch install instructions</th>
<th>Service-interrupting?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IMPORTANT</strong>: Before applying the SP15.3 patch files, refer to the SP15.3 Release Bulletin, section “SP15.3 Additional Notes”. There is a slight change in the order of patching for this release due to the upgraded DB. Failure to follow the steps listed in the bulletin will result in an erroneous DB failure message.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Verification

To verify the OS, DB and Tomcat versions after applying all patches, run the “showversion” command from the primary EM server and ensure the OS, DB and Tomcat versions match those listed in the Release Bulletin.

<table>
<thead>
<tr>
<th>Failure</th>
<th>n/a</th>
</tr>
</thead>
</table>

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.

<table>
<thead>
<tr>
<th>Security risks</th>
<th>n/a</th>
</tr>
</thead>
</table>

Avaya Security Vulnerability Classification

Not Susceptible

<table>
<thead>
<tr>
<th>Mitigation</th>
<th>n/a</th>
</tr>
</thead>
</table>

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 owner.