Product Support Notice

© 2015 Avaya Inc. All Rights Reserved.

PSN #	PSN004440u				
Original publication date: 04-Mar-15. This is Issue #03, published date: 31-Mar-15.		Severity/risk level	High	Urgency	Immediately
Name of problem	AS5300 SP10.1 IA (Security) Patch				

Products affected

Avaya Aura® Application Server 5300 (AS 5300) Release: 3.0 SP9 and 3.0 SP10

Problem description

Several critical security vulnerabilities that were reported in the Jan 2015 IAVAs in the area of:

- Red Hat Enterprise Linux OS
- JAVA/JRE
- Postgres database
- MySQL database

Resolution

AS 5300 R3.0 SP10.1 is a security-only patch that impacts the AS 5300 core Linux platform, the Postgres database (embedded in the AS 5300 SIP Core applications), and MySQL database (embedded in the Avaya Media Server).

AS 5300 R3.0 SP10.1 does NOT contain bug fixes related to IO (Interoperability) or call services/features. As a result, the AS 5300 R3.0 SP10.1 patch does NOT include a new AS 5300 Core Application patch.

For systems running AS 5300 R3.0 SP9 or older: Customers must upgrade the system to SP10 before applying the patches delivered in SP10.1. SP10.1 patches must be applied per the patch procedure outlined in the Patch Notes of this PSN.

For SP10 systems: Customers should apply the SP10.1 patches per the patch procedure outlined in the Patch Notes of this PSN.

The following paragraphs list the updates contained in AS 5300 R3.0 SP10.1, along with the security vulnerabilities that it resolves as a reference:

MySQL is updated to v5.5.41 in the Avaya Media Server 7.5 platform which resolves the following vulnerabilities/CVEs:
Filename: MCP_MediaServer_7.5.0.1297_2015.01.27_1032.zip

- CVE-2015-0411
- CVE-2015-0382
- CVE-2015-0381
- CVE-2015-0432
- CVE-2014-6568
- CVE-2015-0374

PostgreSQL is updated to 9.0.19-17 which resolves the following vulnerabilities/CVEs in the SIP Core Postgres database:
Filename: installer-mcp-postgresql-9.0.19-17.AS5300.LINUX64.zip

- CVE-2015-0241 Buffer overruns in "to_char" functions.
- CVE-2015-0242 Buffer overrun in replacement printf family of functions.
- CVE-2015-0243 Memory errors in functions in the pgcrypto extension.
- CVE-2015-0244 An error in extended protocol message reading.
- CVE-2014-8161 Constraint violation errors can cause display of values in columns which the user would not normally have rights to see.

Platform Patch is updated to 15.0.48 which resolves the following Red Hat Enterprise Linux OS Platform vulnerabilities:
Filename: mcp_core_linux_ple2-15.0.48.patches.r-1.ext.iso

****
* Platform release: mcp_core_linux_ple2-15.0.48
****
- Patch: 15.0.47.p-1 (v1.0)

- Updated the main JRE on the system from jre6u85 (jre-1.6.0_85-fcs) to
  jre6u91 (jre-1.6.0_91-fcs). Custom policy files ("local_policy.jar" and
  "US_export_policy.jar") are retained if previously installed in the
  jre6u85 tree.

- RHEL 5.4 RPM Security updates:

Please refer to Red Hat RHEL5 Server Security Errata Database:
https://rhn.redhat.com/errata/rhel-server-errata-security.html

and Red Hat CVE Database:
https://access.redhat.com/security/cve

(*) Indicates RHSA's that are resolved by versions of RPMs prior to
those updated by this security update (i.e., the security fix is accumulated into the listed package versions).

Packages:
kernel-2.6.18-402.el5.x86_64.rpm
kernel-headers-2.6.18-402.el5.x86_64.rpm

Refer to RHSA-2015-0164 (https://rhn.redhat.com/errata/RHSA-2015-0164.html)
CVE-2014-7822 kernel: splice: lack of generic write checks
https://access.redhat.com/security/cve/CVE-2014-7822

Packages:
kernel-2.6.18-402.el5.x86_64.rpm
kernel-headers-2.6.18-402.el5.x86_64.rpm

Refer to RHSA-2015-0164 (https://rhn.redhat.com/errata/RHSA-2015-0164.html)
CVE-2014-7822 kernel: splice: lack of generic write checks
https://access.redhat.com/security/cve/CVE-2014-7822

Packages:
glibc-2.5-123.el5_11.1.i686.rpm
glibc-2.5-123.el5_11.1.x86_64.rpm
glibc-common-2.5-123.el5_11.1.x86_64.rpm
glibc-headers-2.5-123.el5_11.1.x86_64.rpm
glibc-devel-2.5-123.el5_11.1.i386.rpm
glibc-devel-2.5-123.el5_11.1.x86_64.rpm

Refer to RHSA-2015-0090 (https://rhn.redhat.com/errata/RHSA-2015-0090.html)
CVE-2015-0235 glibc: __nss_hostname_digits_dots() heap-based buffer overflow
https://access.redhat.com/security/cve/CVE-2015-0235

Packages:
tzdata-2015a-1.el5.x86_64.rpm

© 2015 Avaya Inc. All Rights Reserved.

Refer to RHEA-2015:0141-2 (https://rhn.redhat.com/errata/RHEA-2015-0141.html)

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.

Download

AS 5300 R3.0 SP10.1 can be downloaded from the following URL of the Avaya support portal:
https://support.avaya.com/downloads/download-details.action?contentId=C2015361222559270_0&productId=P0626&releaseId=3.0

Patch install instructions	Service-interrupting?
Follow the AS 5300 R3.0 update procedures as documented in 103.1.2 AS 5300 3.0 Software Update MOP to apply ONLY the Linux platform, Postgres database, and Avaya Media Server platform respectively. The high level steps are: Apply the Linux platform patch to each AS 5300 server Apply the Database patch to the primary and secondary DBs Apply the Avaya Media Server (AMS) base platform patch to each AMS server	No

Verification

To check the OS platform version after applying the SP10.1:
Run mcpRelease.pl from user with AA role.
Example output for SP10.1:

*** MCP Platform Release ***

System Type: mcp_core_linux_ple2
Release Level: **15.0.48** (via patching)
Hardware Env: VMware Virtual Machine

To check the PostgreSQL version after applying the SP10.1:
Run dbRelease.pl from user with the DBA role.

Example output for SP10.1:
DB_type = postgresql
DB_version = **9.0.19**
DB_patch = **17**
Replication = symmetric-ds
Replication_version = 2.5.5

To check the AMS version after applying the SP10.1:
Run “cat /etc/mas.properties” on AMS server from user with the root role.

Example output for SP10.1:

© 2015 Avaya Inc. All Rights Reserved.

inst_dir=/var/mcp
installed=yes
mysql=/var/mcp/ma/MAS/platdata/MySQL/
adhoc_app=7.6.0.5
annc_app=7.6.0.5
chat_app=7.6.0.5
meetme_app=7.6.0.5
moh_app=7.6.0.5
ucomm_app=7.6.0.5

mas=7.5.0.1297

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.