Name of problem
AS 5300 R3.0 SP12.3 IPSec with CA3 certificate fails to start

Products affected
Avaya Aura® Application Server 5300 (AS 5300) Release: 3.0 SP11/SP12/SP12.1/SP12.2

Problem description
An IPSec issue was found while installing the DoD CA3 SHA2 certificates, which is preventing IPSec from starting correctly.

Resolution
AS 5300 R3 SP12.3 is an OS patch that fixes an issue with the IPSec daemon when the DoD CA3 SHA2 certificates are used. The problem is not the SHA2 aspect of the certificate, but rather a change to the CRL URI that is only present in the CA3 certificates (and not in the CA2 certificates).

Customers should apply the SP12.3 patch per the patch procedure outlined in the Patch Notes of this PSN.

Once this patch is applied, IPSec will start correctly when certificates (e.g. CA3) with the following CRL URI syntax are used:

X509v3 CRL Distribution Points:
  Full Name:
    URI:http://crl.disa.mil/crl/DODIDSWCA_37.crl

Like most OS patches, the server will be automatically rebooted after the patch is successfully installed.

IPSec will be in the same state after the patch as it was before installing the patch. If it was running before the patch was installed, then it will be restarted after the server is automatically rebooted when the patch is finished installing. If it was stopped before the patch was installed, then it will NOT be running after the server is automatically rebooted when the patch is finished installing.

Note: This PSN is NOT the same as PSN004737u (“AS5300 R3 IPSec Instability after upgrade to SP11”). The hotfix listed in PSN004737u MUST still be applied. The order of the installation of this PSN and PSN004737u does not matter - they can be installed in any order, but both should be applied on all systems.

Workaround or alternative remediation
Until this patch is applied, the DoD CA3 certificates cannot be used for IPSec. It can be used for all other connections, but not for IPSec.

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 platform patch.

Download
The following patch file is found on the AS 5300 R3 SP12.3 support portal webpage.

Platform filename: mcp_core_linux_ple2-15.0.58.patches.r-1.ext.iso
Patch install instructions

Follow the AS 5300 R3.0 update procedures as documented in 103.1.2 AS 5300 3.0 Software Update MOP to apply the Linux platform patch.

The high level step is:

1) Apply the Linux platform patch to every AS 5300 server (both SIP Core and AMS)

Verification

To check the OS platform version after applying the SP12.3 platform patch:

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

```
mcpRelease.pl
```

Example output for SP12.3):

```
[sadsam@server4879-vm01 ~]$ mcpRelease.pl

*** MCP Platform Release ***
System Type:      mcp_core_linux_ple2
Release Level:    15.0.58 (via patching)
Hardware Env:     VMware Virtual Machine
```

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.

Business Partner Notes
Additional information for Business Partners
n/a

Avaya Notes
Additional information for Tier 3, Tier 4, and development
n/a