Server Automation (SA)/Server Automation Virtual Appliance (SAVA) Alert: POODLE: SSLv3 Vulnerability

(November 06, 2014)

ACTION: First, update your SA core server's operating system with a Vendor Patch Release. Then update your Server Automation Core using the instructions below.

Issue that Requires Attention 2
Impact on SA 2
Immediate Mitigation 2

Change Table for this Document

Date	Change
Oct 27, 2014	Initial Release
Nov 06, 2014	SA Virtual Appliance update

Issue that Requires Attention

SSLv3 exposes vulnerability: CVE-2014-3566

The Poodle attack is a MITM (Man in the Middle) vector that allows an attacker to force a *protocol downgrade* between a client and a server. This means both the client and the server will communicate using this downgraded protocol.

Impact on SA (Ultimate Edition) and SA Virtual Appliance (SAVA) (Standard Edition)

General

SA Gateways communicate using only the TLS protocol. This fact mitigates inter-core, slice and agent communication.

The java desktop client and web front end traverse an Apache HTTP server proxy which is configured to allow SSLv3.

SA 9.14 and above Agent-to-Agent communication occurs when using the SA Managed Server Peer Content Caching feature. Agents are allowed to communicate using SSLv3 and there is no way to disallow SSLv3 without redistributing the agent binaries. The problem is somewhat mitigated by the fact there is no cookie or session established during this transaction and therefore nothing for an MITM attacker to gain.

Immediate Mitigation SA

Remove SSLv3 from the httpsProxy/ httpd.conf File

You must edit an entry in the file:

`/etc/opt/opsware/httpsProxy/httpd.conf`

Change the entry:

```
SSLProtocol -ALL +SSLv3 +TLSv1
```

to

```
SSLProtocol -ALL -SSLv3 +TLSv1
```

to disable SSLv3 negotiation (change +SSLv3 to –SSLv3).

Restart the `httpsProxy` component:

```
# service opsware-sas restart httpsProxy
```

Mitigation for SA Virtual Appliance (SAVA) (Standard Edition)

To ensure that this vulnerability will not affect your SA Virtual Appliance (SAVA) system, complete the steps in the following sections.

Download the appliance update

Contact HP Technical Support. You will be granted access to a download that contains an appliance update.

To download and run the fix, go to: **https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/SRVA_00185** and download Patch Update for SA Standard Patch SRVA_00185.zip.

Applying the appliance update

Backup

Backup your SA virtual appliance. See the *SAVA Installation and Administration Guide* for more information.

Update

1. Unzip the archive:

   #unzip SRVA_00185.zip
2. Log into the **appliance** using the Administrator account and its associated password.
3. From the *Actions* menu, select the *Update appliance* option.
4. Click *Upload file* button and in the resulting directory/file browse window.
5. Select the appliance update file: sastd_rollup_10.02.003_52600.bin that you downloaded in the *Download the appliance update* step.
6. Accept and acknowledge all the following confirmation requests so that the appliance update process can start.
7. When the update completes, the appliance will restart.
8. After successful bin update the appliance version should display as 7.2.0-52600.