AI Alert:
POODLE: SSLv3 Vulnerability

(September 10, 2015)

ACTION: Update AI core with the documented instruction.
The information in this alert should be acted upon right away.

Change Table for this Document

Date	Change
Oct 27, 2014	Initial Release
Sep 10, 2015	1. Added AI Database- Vertica Mitigation steps 2. Changed the File name for this bulletin

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 server.   This means both the client and the server must be able to communicate with this downgraded protocol.

Impact on AI

General

The AI Core is the platform management center for an AI system. It has an Apache HTTP Server shielding the Services on the core.

Communication occurs through this HTTP server gateway. The HTTP server receives packets on port 4443 from web UI requests, REST API calls and data miners that interact with AI core. Port 4443 also accepts SSLv3 packets.

HP AI database -Vertica 6.1.3 running SSLv3 is found to be vulnerable.

Immediate Mitigation

Remove SSLv3 from the HTTP Server configuration

AI Core

1. Modify the HTTP server (gateway) configuration file:

/etc/opt/HP/CBI/http/extra/httpd-ssl.conf

Change the SSLProtocol property (Line 90) to remove support for SSLv3 protocol

Sample **httpd-ssl.conf** entry:

```
# SSL Protocol support:
# List the protocol versions which clients are allowed to
# connect with. Disable SSLv2 by default (cf. RFC 6176).
SSLProtocol all -SSLv2
```

In the above property configuration append the string -SSLv3

The updated configuration should look like the following:

```
# SSL Protocol support:
# List the protocol versions which clients are allowed to
# connect with. Disable SSLv2 by default (cf. RFC 6176).
```

SSLProtocol all -SSLv2 -SSLv3

2. Restart the Gateway service on the AI core:

# /etc/init.d/cbid restart gateway

AI Database- Vertica Core

HP AI recommends installing/Upgrading to Vertica v7.1.2-1 or subsequent. Instructions for downloading and installing/upgrading Vertica 7.1.2-x are available at SSO

1. Logon to SSO Portal using HP Passport credentials.
2. Download the **AI_00001.zip** Patch.
3. The Vertica 7.1.2-x package and instructions document to upgrade is uploaded to SSO-AI_00001.zip for downloads.
4. It's available at **ftp://quixy.deu.hp.com/mv_patches/AI/AI_00001.zip**.
5. The patch is also available on the SSO Portal at: **https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/AI_00001**

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither HP or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Hewlett-Packard Company and the names of Hewlett-Packard products referenced herein are trademarks of Hewlett-Packard Company in the United States and other countries. Other product and company names mentioned herein may be trademarks of their respective owners.