Asset Manager and the Heartbleed Vulnerability (CVE-2014-0160)

Revision 1.0

As of: April 18, 2014

Table of Contents

Situation Overview

Per the HP Software bulletin, certain versions of the HP Asset Manager product were affected by the Heartbleed vulnerability present in the third party OpenSSL library.

Depending on your configuration, you may be impacted (details at the above bulletin and below). Per the bulletin, the following versions of Asset Manager include the version of OpenSSL that was found vulnerable. The product versions are:

- HP Asset Manager 9.40 (including all patches)
- HP Cloud System Chargeback 9.40 (including all patches)

To remove any doubt, the following Asset Manager Product versions were NOT AFFECTED by the Heartbleed vulnerability:

- HP Asset Manager 5.20, 5.21 and 5.22(including all patches)
- HP Asset Manager 9.30, 9.31 and 9.32(including all patches)

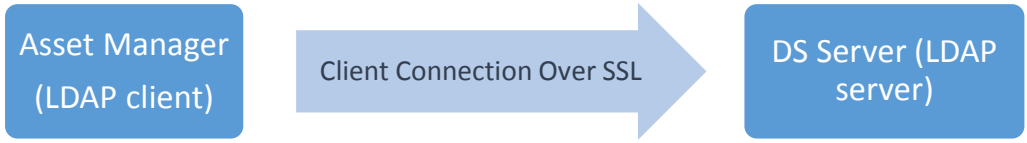
Note: Regardless of the versions listed above, you may still be vulnerable, depending on 3rd party products that are used for the deployment of Asset Manager. Please see Appendix A for further details.

HP is not responsible for supporting 3rd party components used to deploy its products and you should treat the guidelines available in Appendix A as recommendations only – for further instructions it is recommended to consult with the 3rd party component vendor.

Clarification on the vulnerability applicability

Asset Manager uses OpenSSL to connect to Directory Services Server via the secure LDAP protocol. Secure LDAP is also known as LDAP over SSL (LDAPS). Examples of Directory Services ("DS") servers are Microsoft Active Directory and Novell eDirectory.

Even if using the impacted Asset Manager versions stated above, your Asset Manager deployment is directly impacted only in cases where the AM database is configured to integrate with LDAP using Secure LDAP protocol as illustrated in the diagram below:



Asset Manager that are not integrated with LDAP or are integrated with LDAP using an unsecure connection are not affected by the vulnerability even if using an affected version.

In addition, please take into consideration that in case the Asset Manager and the DS Server are implemented within an organization's intranet, any possible exploit of the vulnerability must result from attacks originating within the network.

Recommended mitigation plan

If your organization's architecture is similar to the above, in order to minimize your exposure to the vulnerability you can take the following action until HP releases a fix to the vulnerability:

Determine the security of the network infrastructure between Asset Manager and the DS Sever. Consider whether implementing one or more proxy LDAP severs will mitigate any risks.

Recommended action plan

1. Consult with the vendor of your Directory Services server to confirm whether it uses vulnerable versions of OpenSSL. If so, follow the recommendations from the vendor to fix the vulnerability.
2. Apply a newer version of Asset Manager which resolves the vulnerability.

Note: The following are follow-up actions that may be required after the environment has been fully patched:

- Generate new keys and certificates for your Directory Services Server (and proxies as required).
- Generate new SSL certificates for use by the HP Asset Manager so that the LDAPS integration to your Directory Services Server is functional.
- Change passwords for all HP Asset Manager users/operators on DS server.

The attack vector on Asset Manager itself is smaller than that of the Directory Server given that AM is acting only as a client. You may search for “reverse heartbleed” for more information.

Appendix A

HP Asset Manager – Using LDAP Proxy Server

Organizations where the DS server is not within the same network as the AM, or that have architectures similar to the following, are also exposed to the vulnerability:

For this scenario, see the action plan above and consider firewall(s), proxy server(s) and the DS server itself in the action plan.

HP CloudSystem Chargeback Embedded Tomcat Components

The HP CouldSystem Chargeback ships a version of Tomcat that has no HTTPS connectors enabled default. Therefore, out of the box installations are not affected.

However, if you reconfigured or customized the HTTPS connector to use the Apache Portable Runtime or APR (HP does not recommend or document how to do this) you may be impacted. For example, if both of the following lines exist in your customized AM CloudSystem Chargeback's Tomcat server.xml, you will be affected by the OpenSSL issue:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
<!-- Define a APR SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector protocol="org.apache.coyote.http11.Http11AprProtocol" port="8443" .../>
```

If you have customized the configuration as noted above, the proposed solution is to remove the APR line in server.xml as mentioned below:

1. Navigate to the server .xml file.

   <AM_Dir>/tomcat_webservice/conf/server.xml
   and
   <AM_Dir>/tomcat_webtier/conf/server.xml

2. Remove or comment out the following line from the file:

   <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="off" />

3. Change HTTPS connectors configuration as following:

   from
   <Connector protocol="org.apache.coyote.http11.Http11AprProtocol" port="8443" .../>

   to
   <Connector protocol="org.apache.coyote.http11.Http11Protocol" port="8443" .../>

4. Restart Tomcat.
5. Revoke the server certificates that are used in Tomcat and generate new ones.