HP Configuration Manager and HP UCMDB Browser and the Heartbleed Vulnerability (CVE-2014-0160)

Revision 1.0
As of: April 17, 2014

Table of Contents

Situation Overview

Per the HP Software bulletin, certain versions of the HP Configuration Manager and HP UCMDB Browser are 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 CM and UCMDB Browser include the version of OpenSSL that was found vulnerable. The product versions are:

- Configuration Manager 9.1x, 9.2x, 9.3x, 10.01, 10.10 (including all patches)
- UCMDB Browser (with Tomcat embedded install bits) 1.x, 2.x, 3.x

The following setups are NOT AFFECTED by the Heartbleed vulnerability:

- Out-of-the-box CM and UCMDB Browser configurations;
- CM and UCMDB Browser configurations that were performed according to the official deployment and installation documentation;
- Any UCMDB deployment.

Note: Regardless of the versions listed above, you may still be vulnerable, depending on 3rd party products that are used in conjunction with HP UCMDB, CM, or UCMDB Browser. 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

Both UCMDB Browser and CM use a bundled Tomcat web server that includes OpenSSL. Even if using the impacted CM or UCMDB Browser versions stated above, your deployment is only affected in case you have configured the Tomcat server to use APR SSL connectors. In addition, please consider that if the product is only accessible from an organization's intranet, any possible exploit of the vulnerability must result from attacks originating within the network.

UCMDB can be deployed with a PostgreSQL database that is bundled with the installer. While the bundled PostgreSQL includes the vulnerable OpenSSL library, the UCMDB deployment is not affected by the Heartbleed vulnerability because the bundled PostgreSQL is always installed on the same machine as UCMDB, and it is not using SSL.

For UCMDB deployments where the customer uses a remote PostgreSQL database, the database may be affected by the vulnerability if it is using OpenSSL connectors. Customers can remove the vulnerability by deploying a newer PostgreSQL version, or by following instructions provided by the 3rd party component vendor to stop using the OpenSSL connectors.

Universal Discovery is deployed with a PostgreSQL database that is bundled with the installer. While the bundled PostgreSQL includes the vulnerable OpenSSL library, the Universal Discovery deployment is not affected by the Heartbleed vulnerability because the bundled PostgreSQL is always installed on the same machine as Universal Discovery Probe, and it is not using SSL.

Recommended mitigation plan

If your Tomcat web servers have been configured to use APR SSL connectors, you can remove the risks of the Heartbleed vulnerability by replacing the APR SSL connectors with JSSE SSL connectors (see appendix B).

Recommended action plan if vulnerability is applicable

1. Follow the mitigation plan
2. Apply newer versions of UCMDB Browser and Configuration Manager.

Note: The following are follow-up actions that may be required after the environment has been upgraded OR the mitigation steps were taken:

- Generate new keys and certificates for your Tomcat hosting CM or UCMDB Browser.
- Revoke the server certificates that were used in Tomcat.
- Change HP UCMDB users passwords.

Appendix A

Load Balancer and Reverse Proxy

HP UCMDB, CM and UCMDB Browser can be deployed behind a load balancer or reverse proxy that may leverage OpenSSL.

Your load balancer/reverse proxy may be impacted if it uses a vulnerable version of OpenSSL. Please see the official vulnerability details for the affected versions, and consult the manufacturer of your device to determine

whether you are impacted. If you are using a vulnerable version, you should follow the recommended steps provided by the official vulnerability information and your vendor.

Remote PostgreSQL installation

If you are using a remote PostgreSQL installation with UCMDB or Universal Discovery, and that installation leverages an OpenSSL connector, please follow the vendor's mitigation plan for PostgreSQL.

Appendix B

Securing vulnerable Tomcat configurations

CM:

1. **Go to** *<CM_Dir>/servers/server-0/confserver.xml*
2. **Remove below line from the file:**
   <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="off" />
3. **Change HTTPS connectors configuration**
   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 used in Tomcat**

UCMDB Browser:

1. **Go to** *<Browser Install Dir>/conf/server.xml*
2. **Comment out below line in the file**
   <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
3. **Change HTTPS connectors configuration**
   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 used in Tomcat**