Hewlett Packard
Enterprise

HPE Software Security Update

HPE UCMDB Configuration Manager

OpenSSL May 3rd 2016 Vulnerability

CVE – 2016 - 2108

CVE – 2016 - 2107

Date	Version	Change
October 12, 2016	Version 1.0	Initial release

Summary:

The following article provides information regarding the OpenSSL May 3rd 2016 Vulnerability.

Topic

A new set of security vulnerabilities were published by the OpenSSL group on May 3rd 2016.

Detail can be found in the following link: **https://www.openssl.org/news/secadv/20160503.txt**
Out of several security vulnerabilities, 2 were reported as High CVE issues and require the update of the OpenSSL version, if one is affected.

1. Memory corruption in the ASN.1 encoder (CVE-2016-2108)

2. Padding oracle in AES-NI CBC MAC check (CVE-2016-2107)

Affected Releases:

The following versions of HPE Universal CMDB were found vulnerable:

UCMDB Configuration Manager 10.10 / 10.11
UCMDB Configuration Manager 10.20

ACTION: Review all details in instructions provided in this paper to address the vulnerability.
HPE SW recommend to address this information as soon as possible.

Response

Impact on HPE UCMDB Configuration Manager

HPE UCMDB Configuration Manager is affected.

Secured communication between UCMDB server and CM/ CM and client may be affected. TLS session could be decrypted and sensitive information retrieved.

Mitigation Actions

HPE has released the following software updates to resolve the vulnerability for the impacted versions of HPE UCMDB Configuration Manager:

Note: HPE recommends installing the latest software updates, if possible. Customers unable to apply the updates should contact HPE Support to discuss options.

Affected versions	Solution	
HPE UCMDB CM 10.10, 10.11	HPE UCMDB CM 10.11 CUP8 or later Windows: **https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00183** Linux: **https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00184** Re-run the configuration by following one of the steps, as described in **Appendix A**	
HPE UCMDB CM 10.20	HPE UCMDB CM 10.21 or later Windows: **https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00163** Linux: **https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00164**	

	Re-run the configuration by following one of the steps, as described in Appendix A	

Appendix A

CM acting as a server

Each version of CM has an embedded Tomcat server which handles SSL/TLS requests. In order to disable this protocol, follow the steps such as:

1) Stop CM
2) In installation folder locate the following file: tomcat/conf/server.xml and servers/server-0/conf/server.xml
3) In each of the two files above, if the HTTPS connector is enabled add the following sslProtocols ="TLSv1,TLSv1.1,TLSv1.2" to that connector

   It should look like this:

   ```
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
   maxThreads="150"SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
   sslProtocols ="TLSv1,TLSv1.1,TLSv1.2" />
   ```

Hewlett-Packard Enterprise 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 HPE 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 Enterprise products referenced herein are trademarks of Hewlett-Packard Enterprise Company in the United States and other countries. Other product and company names mentioned herein may be trademarks of their respective owners.