Hewlett Packard Enterprise

HPE Software Security Update

HPE UCMDB Configuration Manager

DROWN SSLv2 - CVE-2016-0800 Vulnerability

Date	Version	Change
October 12, 2016	Version 1.0	Initial release

Summary:

The following article provides information regarding the DROWN SSLv2 Vulnerability.

Topic

Vulnerability in SSLv2 protocol which being referred to as DROWN – **D**ecrypting **R**SA using **O**bsolete and **W**eakened e**N**cryption. This vulnerability in SSLv2 allows attackers **to decrypt TLS** sessions without the knowledge of the matching private RSA key.

In this vulnerability, an attacker using this flaw and an active man-in-the-middle (MITM) attack can impersonate a TLS server to connecting TLS client, decrypt recorded SSL/TLS sessions and obtain sensitive data from the decrypted session including authentication credentials

This flaw can be exploited to decrypt secure sessions using the TLS (v1.0-1.2) protocol.

The flaw can be divided to 3 parts:

1. "General DROWN" in SSLv2 Protocol (CVE-2016-0800)

The new cross-protocol attack allows decryption of SSL/TLS sessions even if one is using **TLS** (1.0 - 1.2), by abusing this SSLv2 weakness.

DROWN shows that merely supporting SSLv2 is a threat to modern servers and clients. It allows an attacker to decrypt modern TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key. Web-applications, Websites, mail servers, instant messaging services and other SSLv2-dependent services that share the same private keys with HPE SW products may pose a risk to our customers.

2. "Special DROWN" in OpenSSL (CVE-2016-0703, CVE-2016-0704)

Additionally, flaws were found in the SSLv2 protocol implementation in OpenSSL cryptography and SSL/TLS library, which make it possible to perform a more efficient variant of the DROWN attack, referred to as "special DROWN".

3. CVE-2015-3197 (old CVE) + DROWN (CVE-2016-0800)

In this scenario, a correlation between a CVE found in OpenSSL + DROWN creates a major threat when using OpenSSL.

If a product implements OpenSSL, versions prior to 1.0.2f and 1.0.1r, it will allow a DROWN attacker to connect to the server with disabled SSLv2 cipher suites, provided that support for SSLv2 itself was not disabled via **SSL_OP_NO_SSLv2**.

Vulnerability Origin:

1. The HPE SW product's configuration allows SSLv2 connections.

2. The HPE SW product allows SSLv2 connections due a bug in OpenSSL versions prior to

1.0.1r / 1.0.2f (CVE-2015-3197).

3. The HPE SW product shares the same RSA private key with a 3rd party service that allows

SSLv2 connection. (Using the same private key for the product.)

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 HPE UCMDB Server and HPE UCMDB Configuration Manager/ HPE UCMDB Configuration Manager 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" />