

HPE Software Security Update

HPE Universal CMDB

DROWN SSLv2 - CVE-2016-0800 Vulnerability

Date	Version	Change
October 7, 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**bssolete and **W**eakened eNcryption. 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 10.10 / 10.11

UCMDB 10.20 / 10.21

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 Universal CMDB

The Universal CMDB Server component of UCMDB, is affected.

The DDM Content Pack component of UCMDB, is affected.

Secured communication between server and clients/ server and probe/ probe and agents 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 Universal CMDB:

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 10.10, 10.11	HPE UCMDB 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 DDM Content Pack 19 Version 19.00 https://hpln.hpe.com/contentoffering/ud-content-packs	
HPE UCMDB 10.20, 10.21	HPE UCMDB 10.22 Windows: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00165 Linux: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00166 DDM Content Pack 19 Version 19.00 https://hpln.hpe.com/contentoffering/ud-content-packs	

©Copyright 2015 Hewlett-Packard Enterprise Development Company, L.P.

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.