Security Update - Customer Announcement

Subject: DROWN vulnerability (CVE-2016-0800) – Updated March 6, 2016

Overview

Ex Libris has been made aware of a recently discovered vulnerability known as DROWN (Decrypting RSA with Obsolete and Weakened Encryption) that affects HTTPS and other services that rely on SSL/TLS implementations and is rated as "High".

An unauthorized user can execute this vulnerability to read or steal information sent via the 'secure connection' by decrypting the SSL session. The attack will succeed as long as the targeted system supports the SSLv2, even if the system is not running SSLv2. This flaw is in the SSLv2 protocol, and affects all implementations.

A server is vulnerable to a DROWN attack if either of the following two conditions are met:

1. It supports SSLv2 requests
2. Its private key is used on any other server that allows SSLv2 connections, even for newer SSL/TLS protocol versions

Detailed information about this vulnerability can be found in the Red Hat advisory CVE-2016-0800 where more information is available.

Additional references

More detailed analysis of this vulnerability is available from:

- https://access.redhat.com/articles/2176731
- https://drownattack.com/
- https://www.us-cert.gov/ncas/current-activity/2016/03/01/SSLv2-DROWN-Attack

Effective Security Severity Level: High

Affected Systems: Ex Libris products using SSL traffic (HTTPS) where SSLv2 is still enabled.

Tests and Certifications: The mitigation for this vulnerability has been identified and tested and certified for Ex Libris products.

Actions Taken for Hosted Systems: Ex Libris cloud is protected from this vulnerability.

Required Actions for On-Premises and Local Systems:

Ex Libris strongly recommends the following:

1) Apply the latest 3rd party update using Util SP command as explained in the Ex Libris article.

2) As a best practice, add the following mitigation:
   1) Back up the Apache ssl.conf file
   2) Update the ssl.conf file with the following lines:
      a. SSLProtocol all -SSLv2 -SSLv3
      b. SSLHonorCipherOrder on
      c. Replace the SSLCipherSuite setting with the following:

```
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-
SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-
AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-
SHA:ECDHE-ECDSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-
CBC3-
SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-
DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA
```