DROWN vulnerability (CVE-2016-0800)

How to avoid 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”.

- **Product:** Aleph
- **Product Version:** 21,22,23
- **Relevant for Installation Type:** Dedicated-Direct, Direct, Local, Total Care

Description

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

Resolution

The Ex Libris Security Officer has published an announcement regarding this vulnerability and its solution: Security Update Customer Announcement - DROWN Security Vulnerability.pdf

- **Article last edited:** 08-March-2016