Ex Libris Security Update

Subject: Ex Libris Patron Directory Services (PDS) Security vulnerability

Updated: July 8, 2016

Overview

A Critical ranked vulnerability has been discovered in Ex Libris PDS component.

PDS is used to integrated Ex Libris products with the institutional identity management systems (LDAP, Shibboleth, etc.).

The vulnerability, if exploit by an attacker, may compromise the security level of PDS.

Effective Security Severity Level: Critical

Affected Systems: Ex Libris' locally installed products that are using PDS: Aleph, Voyager, DigiTool, Primo, MetaLib, Rosetta, and Verde.

Tests and Certifications: The HF for this vulnerability has been developed, tested and certified for all of Ex Libris products that are using PDS.

Actions Taken for Hosted Systems: Ex Libris has already deployed the fix to all of the cloud environments and no action is required by our cloud customers

Immediate Actions Required for Locally Installed PDS:

Ex Libris is asking customers to implement the fix as soon as possible, according to the below instructions:

1. Log into the PDS server as the relevant application user (aleph/primo/metalib etc...)
2. Restart apache – **Make sure apache restart was successful before moving on to the next step.**
3. Execute the following commands:
   a. pdsroot; cd program
   b. wget --connect-timeout=60 ftp://produser:Pr6gue@ftp.exlibrisgroup.com/product_patches/PDSupdate ./
   c. tar -zxvf PDSupdate
   d. ./RunMe.sh
4. restart apache