SSL 3.0 Vulnerability ("POODLE")

- **Product:** Cross-Product
- **Product Version:** All

Description

Engineers at Google have disclosed a vulnerability in SSLv3 that can allow a network attacker to decrypt the contents of certain encrypted web communications.

The exploit is called POODLE (Padding Oracle On Downgraded Legacy Encryption) (CVE-2014-3566), and is made possible by the abuse of a deprecated encryption protocol included in most web browsers and web servers, for legacy site and/or browser compatibility.

The Ex Libris Security Officer has published an announcement regarding this vulnerability: Security Update Customer Announcement-Poodle.pdf

Resolution

Products Metalib, Aleph, DigiTool and Alma have been successfully tested with the following solution:

1. In ssl.conf, add the following line after the current SSLCipherSuite directive:

```
#   SSL Cipher Suite:List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
SSLProtocol All -SSLv2 -SSLv3
```

2. Restart Apache, which will start apache https without support for SSLv2 and v3 which are vulnerable for the latest security issue.

Additional Information

Specific to Aleph:

- The ssl.conf file is located in ./alephe/apache/conf
- Use util w/3/6 to restart the Apache server.
- On Dec. 10, 2014, rep_change 2114 was added to Aleph 22: Remove support for SSLv2 and SSLv3 (which are vulnerable).

- **Article last edited:** 11-Dec-2014