ExLibris The bridge to knowledge

# Security Update Customer Announcement

## Subject: "POODLE" – The SSL v3 Security vulnerability update

## Overview

Ex Libris has been made aware of a recently discovered a vulnerability that dubbed "POODLE".

A bug has been found in the Secure Sockets Layer (SSL) 3.0 cryptography protocol (SSLv3) which could be exploited to intercept data that's supposed to be encrypted between clients and servers.

This vulnerability allows man-in-the-middle, such as a malicious Wi-Fi hotspot or a compromised ISP, to extract data from secure HTTP connections.

The vulnerability depends on the fact that most Web servers and Web browsers allow the use of the obsolete SSL version 3.0 protocol to secure their communications. Although SSL has been superseded by Transport Layer Security (TLS 1.2 is the latest published version of the protocol), it's still widely supported on both servers and clients alike and is still required for compatibility with legacy systems.

TLS 1.0 and newer versions perform more robust validation of the decrypted data and as such are not susceptible to the same problem.

The vulnerability is covered by two NIST advisories in the National Vulnerability Database CVE-2014-3566 where more information is available.

Risk Level: NIST rate is as medium.

In addition more detailed analysis of the vulnerability is available from RedHat - https://access.redhat.com/articles/1232123 and Symantec- http://www.symantec.com/connect/blogs/ssl-30-vulnerability-poodle-bug-aka-poodlebleed

## Effective Security Severity level: Medium

**Affected systems**: All systems/products that are using SSL certificate.

## How do I know if I have an SSL certificate on my Ex Libris product?

1. Examine the URL of the website on the address bar of your Web browser. A website with SSL certificate has an URL that starts with "https" instead of the usual "http."

2. Notice an icon that looks like a lock at the left hand side of the address bar of your Web browser. You may also find it at the lower-right of the browser window. Double-click on it to see the website security certificate. It should say "Secured Socket layer (SSL)" somewhere.

**Immediate remediation:** The vulnerability described above requires an SSL 3.0 connection to be established, so disabling the SSL 3.0 protocol in the client or in the server (or both) will completely avoid it.

To mitigate this vulnerability, it is recommended that you explicitly disable SSL 3.0 on all servers running Ex Libris systems/products. It is important to know that if the library users are using the latest browser versions, typically the browser will use TLS encryption mechanism, and not the vulnerable SSL v3 encryption mechanism.

**Tests and certifications:** Ex Libris is in the process of evaluating all Ex Libris products for potential vulnerability and performing certification testing after disabling SSL 3.0 with all Ex Libris systems/products.

**Actions to be taken for Hosted systems:** Ex Libris will deploy the required configuration to all Ex Libris cloud servers once all Ex Libris products will be fully tested and passed certification testing.

**Required action for on-premise/local systems:**

Once all Ex Libris products passed the certification testing, Ex Libris will recommend the customers with on-premise/local systems to follow their server's vendor instructions, and disable SSL 3.0.

Best Regards,

Tomer Shemesh, Ex Libris Security Officer