Ex Libris Response Policy for

Third Party Software Components and Security Patches of Ex Libris Products

January 2012

CONFIDENTIAL INFORMATION

DISCLAIMER

TRADEMARKS

Document updated: January 2012

Web address: http://www.exlibrisgroup.com

January 2012

1. Introduction

Ex Libris considers the security of its products a high priority. As such, Ex Libris continually seeks to ensure that its solutions do not contain vulnerabilities that may compromise the security of its products.

As part of ongoing efforts by Ex Libris to provide secured solutions that help customers maintain the integrity of their environment, the company has implemented a security response process for third party software components used with Ex Libris products and security patches and vulnerabilities.

This security response process comprises of four stages: **Monitoring**, **Assessment**, **Remediation,** and **Communication**. These stages are explained below.

2. Monitoring

Underlying the entire security response process, the security evaluation team—led by the Ex Libris Security Officer—continuously monitors and evaluates the security of Ex Libris products, as well as third-party releases and patches. This ongoing monitoring ensures a fast response when security issues arise. The team proactively tracks new third party releases and roadmap announcements together with security alerts and patches, ensuring a consistently rapid response and proactive approach to products' security.

The list of Ex Libris products and third party software covered in this policy can be found in appendix A1 and A2 of this policy.

3. Assessment

3.1. Third Party Software Components

Each new third party software version is assessed by Ex Libris to determine its suitability to the functionality, stability, and security of the relevant Ex Libris products. Based on this third party software assessment, a decision is made with respect to the third party software version to be certified.

3.2. Third Party Security patches and Ex Libris Products Vulnerabilities

Ex Libris assesses each new security patch and any vulnerabilities found in its products, and categorizes them according to severity using the **Common Vulnerability Scoring System** (CVSS), an industry standard for assessing the severity of computer system security vulnerabilities (www.first.org/cvss/cvss-guide).

The severity level—Critical, High, Medium, or Low—is determined according to the third party vendor's patch severity and its relevancy to Ex Libris products. Further information on security severity scoring can be found in Appendix B of this policy.

4. Remediation

4.1. Third Party Software Components

- All new versions of the third party software listed in appendix A2, will be evaluated.

- **Within three months of** the official third party new version release, Ex Libris will conduct an evaluation of the new version's stability and suitability to the product's needs. The evaluation will be led by Ex Libris CTO, with support from engineering, product management and the security officer.

- If approved, new third party versions will be certified and incorporated in the **next minor or major release** of the relevant product.

- If the new version is not approved, Ex Libris will re-evaluate the release in the next assessment cycle, typically at six month intervals, in view of updates that may be provided by the third party vendor.

4.2.Third Party Security Patches and Ex Libris Product Vulnerabilities

Following the Assessment phase, each security patch or vulnerability is assigned a risk level. Depending on the severity level, Ex Libris will provide the following mitigation actions, described in the table below.

For some third party security patches and vulnerabilities, Ex Libris may recommend configuration changes rather than patch installation, as described in the table below.

Classification Of Severity Level	Remediation Action
Critical Critical severity patches and reported vulnerabilities will be **assessed as soon as possible** (within five business days): • after the official release by the third party vendor, or • from the moment they were reported to or discovered by Ex Libris Security Officer	**Announcement of the availability of Ex Libris provided Hot Fix or patch as soon as possible** **Or** **recommendation for configuration changes**
High and Medium High and Medium severity security patches and reported vulnerabilities will be **assessed** within **two weeks:** • from their official release by the third party vendor or • from the moment they were reported to or discovered by Ex Libris Security Officer	**Incorporate the fix into next service pack** **Or** **recommendation for configuration changes**
Low Low severity security patches and reported vulnerabilities will be assessed within **one month:** • from their official release by the third party vendor or • from the moment they were reported to or discovered by Ex Libris Security Officer	**Incorporate the fix into next minor or major release** **Or** **recommendation for configuration changes**

4.3. Operating Systems' Critical Security Patches

Ex Libris policy with respect to approval and installation of critical security updates issued by Operating Systems (OS) is different than the policy above for third party software.

In the experience of Ex Libris, the likelihood of issues arising following installation of **critical security patches** for **Operating Systems** is very low. Customers may, therefore, choose to install OS critical security patches prior to the official release of the Ex Libris certification, at their discretion. Based on past experience, Ex Libris does not expect product issues to result from installation of these critical security patches.

Ex Libris does, however, recommend installing and testing these patches on a test server before installing them on a production server. Ex Libris will suggest appropriate courses of action for issues that may occur following the installation of OS critical security patches prior to Ex Libris official certification.

4.4. Oracle Critical Patches Updates (CPU)

Oracle routinely publishes critical patches, some of which pertain to security issues. Ex Libris will evaluate and certify current version products with these patches and will make the Oracle patches (CPU) available twice a year.

5. Communication

Ex Libris will update the customer community on any security issue via a "product security announcement." Product security announcements will be sent to the Product Administrator who is registered in the Ex Libris CRM system. Ex Libris encourages all customers to review the registered Product Administrator to ensure that the right person receives security announcements.

Ex Libris will issue technical notes concerning security patches and certified products. In addition, twice a year Ex Libris will provide an update on the third party software evaluation and plan. The technical notes will be posted on the Ex Libris Documentation Center and in the eService knowledgebase.

6. Reporting Security Issues to Ex Libris

Ex Libris considers the security of its products and services a priority. Customers who encounter or suspect any security issue with the Ex Libris products they use should open a support incident in eService and in addition report the issue to: SecurityOfficer@exlibrisgroup.com.

January 2012

Appendix A1 – Ex Libris Products Covered in the policy

This policy covers the following Ex Libris Products:

1. Aleph
2. Alma
3. bX
4. MetaLib
5. Primo
6. Rosetta
7. SFX
8. Voyager

Products that are not listed above will be given a security response for critical issues on a case by case basis.

January 2012

Appendix A2 –Third Party Software Components Covered in the policy

This policy covers the following third party components used by Ex Libris products:

1. Apache
2. Cognos
3. JBoss
4. MYSQL
5. Oracle
6. Tomcat
7. Operating Systems of the products under this policy (OS list can be found at Ex Libris documentation center)

January 2012

Appendix B – Ex Libris self-calculated CVSS score

CVSS scores are mapped into the following severities:

- Critical
- High
- Medium
- Low

An approximate mapping guideline is as follows:

CVSS score range	Severity in advisory
0 – 2.9	Low
3 – 7.9	High and Medium
8.0 – 10.0	Critical

Below is a summary of the factors which illustrate types of vulnerabilities usually resulting in a specific severity level. Please keep in mind that this rating does not take into account the unique characteristics of your installation.

Severity Level: Critical

Vulnerabilities that score in the Critical range usually include:

- Exploitation of the vulnerability results in root-level compromise of servers or infrastructure devices.
- The information required in order to exploit the vulnerability, such as example code, is widely available to attackers.
- Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions.
- For critical vulnerabilities, is advised that you patch or upgrade as soon as possible, unless you have other mitigating measures in place. For example, if your installation is not accessible from the Internet, this may be a mitigating factor.

Severity Level: High and Medium

Vulnerabilities that score in the High and Medium ranges usually have the following characteristics:

- The vulnerability is difficult to exploit.
- Exploitation does not result in elevated privileges.
- Exploitation does not result in a significant data loss.
- Denial of service vulnerabilities that is difficult to set.
- Exploits that require an attacker to reside on the same local network as the victim.
- Vulnerabilities that affect only nonstandard configurations or obscure applications.
- Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics.
- Vulnerabilities where exploitation provides only very limited access.

Severity Level: Low

- Vulnerabilities in the Low range typically have very little impact on an organization’s business. Exploitation of such vulnerabilities usually requires local or physical system access