ExLibris The bridge to knowledge

Security Update - Customer Announcement

Subject: "Ghost" - Security Vulnerability – Updated January 28, 2015

Overview

Ex Libris has been made aware of a recently discovered a vulnerability called "Ghost".

All Unix/Linux systems that use the `glibc` (a popular command-line shell) are vulnerable to the Ghost vulnerability. GHOST is a buffer overflow bug affecting the `gethostbyname()` and `gethostbyname2()` function calls in the `glibc` library. This vulnerability allows a remote attacker to execute arbitrary code with the permissions of the user running the application. The vulnerability is covered by Red Hat advisory CVE-2015-0235 where more information is available.

Patches have been released to fix this vulnerability by major Linux vendors for affected versions.

No Impact to Customer data.

Effective Security Severity level

Critical

Affected Systems

All Ex Libris systems and products running on Linux.

Tests and Certifications

Ex Libris has evaluated Ex Libris products for potential vulnerability and performed certification testing with the available patches for all Ex Libris systems and products running on Linux. It was determined that the available patches can be safely deployed with no impact to Ex Libris systems and products.

Actions Taken for Hosted Systems

Ex Libris is in the process of patching all of the systems running in the Ex Libris cloud and expects to finish this task shortly.

Required Actions for on-Premise/Local Systems

Ex Libris strongly recommends following the vendor's instructions and installing the patch on all on-premise (local) Ex Libris products using Linux systems.

Procedure for Linux Systems

1. Determine your vulnerability to "Ghost". Check your version of `glibc`. Earlier versions of `glibc` than those listed below are vulnerable:
   - `RH6 glibc -2.12-1.149`
   - `RH5 glibc-2.5-123`

For more information, see: https://access.redhat.com/security/cve/CVE-2015-0235

2. Mitigate the vulnerability. If your system is vulnerable, upgrade to the most recent version of the `glibc`. Run the command `yum -y update glibc-*` and install the latest `glibc` version.

Rollback Changes

To roll back the changes in case of a problem, run the command `yum downgrade glibc-*` to revert to your original `glibc` version.

Best regards,

Tomer Shemesh, Ex Libris Security Officer