OpenSSL - Vulnerability "FREAK" (CVE-2015-0204)

- **Article Type:** General
- **Product:** Aleph
- **Product Version:** All

Problem Symptoms:
FREAK was found in TLS/SSL protocol using encryption of Internet communication.
*FREAK(Factoring attack on RSA-EXPORT Keys) is vulnerability that is attributable to export restriction of cryptography from the United States in 1990's.

The site is using OpenSSL. version 0.9.8e.

Is there any influence on ALEPH package?
If yes, we are planning to apply latest patch immediately.

[Reference]
http://www.itmedia.co.jp/enterprise/articles/1503/04/news054.html
http://d.hatena.ne.jp/Kango/20150304/1425448983

Cause:
See Resolution.

Resolution:
Download and install the latest OpenSSL Version (0.9.8zf) with util sp 06 (Download 3rd party products update).

The new version of OpenSSL can be downloaded with util sp:
6. Download 3rd party products update
7. Check 3rd party product download status
8. Extract products updates
9. Update 3rd party soft links
10. Run Third party product OS pre checks

The installation of Third Party tools is not related to the Service Pack schedule.

OpenSSL version 0.9.8zf was provided on the ftp server on 22-March-2015:

openssl-0.9.8zf.Linux.tar.gz

Note that the Third Party download installs all Third Party products, not only OpenSSL.

Additional Information

FREAK is similar to POODLE due to it being vulnerable to potential downgrade attempts with HTTPS traffic between clients and servers.

For more details about certified Third Party tools consult document 'Ex Libris Certified Third-Party Software and Security Patch Release Notes' which can be found in the Ex Libris Documentation Center and is updated quarterly.

Category: System Management (500)

- **Article last edited:** 3/24/2015