FREAK: Vulnerability in SSL and its impact on Seclore FileSecure

What is FREAK?

FREAK stands for Factoring RSA Export Keys & is a newly discovered Man-In-The-Middle (MITM) vulnerability.

Vulnerability CVE

CVE-2015-0204

What is the scope of the vulnerability?

The vulnerability affects systems that allow communication using export grade encryption keys which were limited to 512 bits. A successful MITM attack can force the server to downgrade to export grade keys which are of much lesser strength and can be decrypted with cheaply available computing power.

How does the vulnerability affect my Seclore IRM Infrastructure?

The impact of FREAK vulnerability on your Seclore IRM infrastructure will depend on the SSL endpoint for your IRM infrastructure. The presence of export grade ciphers within the cipher suite configuration would mean that the site is vulnerable to a FREAK attack.

Most SSL endpoints that have been implemented by Seclore, which typically are Apache webserver or FileSecure PolicyServer would not be affected since Seclore does not recommend lower grade encryption keys. For all public facing Policy Server urls, a quick test via either of the following sites should determine the impact of the vulnerability:

https://www.ssllabs.com/ssltest/
https://tools.keycdn.com/freak

What actions are required to mitigate the risk on my Seclore IRM environment?

- For all Apache webserver SSL endpoints, review the cipher suite and eliminate the export ciphers using the !EXP directive within SSLCipherSuite. Additionally, patching OpenSSL is another option to remove the vulnerability:

  OpenSSL 1.0.1 users should upgrade to 1.0.1j.
  OpenSSL 1.0.0 users should upgrade to 1.0.0o.
  OpenSSL 0.9.8 users should upgrade to 0.9.8zc.

- For all Apache Tomcat SSL endpoints, review the cipher suite and remove all EXPORT ciphers which typically include EXPORT as part of the cipher configuration, e.g. TLS_RSA_EXPORT_WITH_RC4_40_MD5.

- In case the SSL endpoint is besides the above servers, please consult with the appropriate vendor support to mitigate any risk related to the vulnerability.

Note: The above advisory is of interim status and shall be updated as new information becomes available. Please reach out to Seclore Support for any additional clarifications.