お客様各位

2014 年 4 月 9 日
ジェイサート株式会社

OpneSSL 脆弱性に伴う、発行済証明書の無償再発行(リキー)措置につきまして

OpenSSL Project が提供する OpenSSL の heartbeat 拡張には情報漏えいの脆弱性があります。悪意ある第三者により、細工したパケットを送付することでシステムのメモリ内の情報を閲覧し、お客様がご利用中の SSL サーバ証明書の秘密鍵等、機密性高い情報を奪取されるリスクがあります。

脆弱性あり、と公知されている OpenSSL のバージョンは次の通りです。

- OpenSSL 1.0.1 から 1.0.1f
- OpenSSL 1.0.2-beta から 1.0.2-beta1

なお、本件はスターフィールド含む SSL サーバ証明書の脆弱性ではありません。 サーバ側環境の問題ですので、詳しくはサーバベンダ・サーバ管理会社にご照会ください。

1. 該当する OpenSSL をご利用中のお客様は、至急、OpenSSL Project が提供する修正済みバージョンへアップデートされることをお勧めします。
   OpenSSL Project
   OpenSSL Security Advisory [07 Apr 2014] - TLS heartbeat read overrun (CVE-2014-0160)
   https://www.openssl.org/news/secadv_20140407.txt

   詳しくは、
   http://www.ipa.go.jp/security/ciadr/vul/20140408-openssl.html
   https://www.jpcert.or.jp/at/2014/at140013.html
   等、Web 上の公開情報をご参照ください。

2. 併せ、弊社より発行済スターフィールド SSL サーバ証明書を、上記により OpenSSL バージョンをアップデートされた後、新たに秘密鍵および CSR(公開鍵)を生成し直し、CSR を弊社までお送りください。無償再発行の措置を取らせて頂きますので、発行済証明書と置換えてください。 詳しくは、support@jcert.co.jp までお問い合わせください。

以 上