2014 年 4 月 21 日
2014 年 5 月 12 日改訂

お客様　各位

日本ストラタステクノロジー株式会社

ストラタス製品における OpenSSL "Heartbleed" 脆弱性 CVE-2014-0160 について

拝啓　貴社益々ご清栄のこととお慶び申し上げます。 また平素より格別のご高配を賜り厚く御礼申し上げます。

首題の件につきまして下記の通りご報告申し上げます。

敬具

記

1. ご案内

多くの製品で使用されているOpenSSL暗号化ライブラリに深刻な脆弱性が見つかりました。この問題は CVE-2014-0160 として報告されており、「Heartbleed」問題とも呼ばれています。このアラート（アラート番号2955）では、各ストラタス製品に対するこの問題の影響とその対応について記述しています。

各ストラタス製品への影響：

Red Hat Enterprise Linuxシステム

- Red Hat Enterprise Linux 6.5が稼働するftServerシステムではこの問題の影響を受けます。
- RedHat Enterprise Linux 6.4及びそれ以前のバージョンはこの問題の影響はありません。

※ただしOpenSSLパッケージを以下のバージョンに変更もしくは更新した場合にはこの問題の影響を受けます。

openssl-1.0.1e-15 以降 openssl-1.0.1e-16.el6_5.4 までのバージョン

- RedHat Enterprise Linux 5 及びそれ以前のバージョンはこの問題の影響はありません。

VMwareシステム

- Automated Uptime Layer 5.1.0.0 がインストールされているESXi 5.5システムではこの問題の影響を受けます。
- Automated Uptime Layer 2.x, 3.x, 4.x 及び 5.0.xがインストールされているシステムはftSysマネジメントアプライアンスを含め、この問題への影響はありません。

（※ただしこれらのシステム上で稼働している仮想マシンは含まない。）

VOSシステム

- 全てのVOSベースのftServerのOpenSSLはバージョン1.0.0もしくはそれ以前のOpenSSLを使用しているためこの問題への影響はありません。

Windowsシステム

- 全てのバージョンのWindowsベースのftServerではOpenSSLを使用していないため、お客様が別途OpenSSLをインストールした場合を除き、この問題への影響はありません。

EverRun及びAvanceシステム

- Avance, EverRun MX, EverRun Enterprise はこの問題への影響はありません。
（※ただしこれらのシステム上で稼働している仮想マシンは含まない。）

VTM

- ftServerシステムに搭載されているバーチャルテクニシャンモジュール(VTM)はこの問題への影響はありません。

ftScalableストレージアレイ及び ftScalableストレージアレイ G2

- ftScalableストレージアレイ及びftScalableストレージアレイG2はこの問題への影響はありません。

問題の要旨：

OpenSSL を使用した TLS および DTLS Heartbeat Extension パケットに情報漏洩の不具合が見つかりました。悪意のある TLS または DTLSクライアントやサーバーは、巧みに作成した TLS または DTLS Heartbeat パケットを、接続しているクライアントまたはサーバーから、必要に応じてメモリ内で限定された場所を開示します。メモリで開示されている箇所は、プライベートキーなど、重要な情報が保存されている可能性があります(CVE-2014-0160)。

２．対応方法

脆弱性の問題が確認されたOpenSSLコンポーネントを使用している場合、この不具合を利用した悪意のあるユーザから攻撃を受ける可能性があります。ご使用中のOpenSSLのバージョンを確認し、該当する場合にはOpenSSLコンポーネントをアップグレードすることを推奨します。この問題とOpenSSLバージョンの関連性は次の通りです。

＊OpenSSL 1.0.1 から 1.0.1f ：影響あり
＊OpenSSL 1.0.1g ：影響なし
＊OpenSSL 1.0.0 ブランチ ：影響なし
＊OpenSSL 0.9.8 ブランチ ：影響なし

VMware社 ESXi 5.5システムへの本問題の対応について

VMware社は以下のナレッジベースにて情報を公開しています。
下記URLの情報にしたがってパッチの適用及び必要な設定を行って下さい。

Resolving OpenSSL Heartbleed for ESXi 5.5 - CVE-2014-0160 (2076665)
http://kb.vmware.com/kb/2076665

現在使用中のOpenSSLパッケージのバージョンを確認する方法は以下の通りです。

Windowsシステムの場合：

[スタート]ボタンをクリックし、[プログラムとファイルの検索]に"cmd"と入力し[Enter]キーを押します。次に表示されたコマンドラインから"openssl /?"と入力します。OpenSSLパッケージがインストールされている場合は、このコマンドによりバージョンが表示されます。

Red Hat Enterprise Linux 6.xシステムの場合：

rpmコマンドを使用して確認します

(実行例)

```
# rpm -q openssl
openssl-1.0.1e-16.el6_5.4.x86_64
```

もしくは以下のコマンドでも確認することができます。

openssl version

この問題に該当するOpenSSLパッケージが確認された場合には、OpenSSLパッケージを openssl-1.0.1e-16.el6_5.7 (RHSA-2014:0376) もしくはそれ以降のバージョンへアップグレードすることを強く推奨致します。尚、アップグレードはOpenSSLライブラリに関係する全てのサービスに影響するため、システムの再起動を伴います。

VMware, Avance, EverRun上で稼働しているLinuxベースの仮想マシン及び、OpenSSLをインストールしたWindowsベースの仮想マシンも、OpenSSLパッケージのバージョンを確認し、適切なバージョンへアップグレードをする必要があります。各ゲストOSの上での確認方法及びアップグレードの方法についてはご契約先の保守窓口へお問い合わせ下さい。

3. 関連情報

Red Hat Enteprise Linux上でのこの問題の詳細については、以下のURLをご参照下さい。

http://rhn.redhat.com/errata/RHSA-2014-0376.html もしくは
https://access.redhat.com/site/solutions/781793

関連ドキュメントURL：
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
http://www.openssl.org/news/secadv_20140407.txt (published 7th of April 2014, ~17:30 UTC)
http://heartbleed.com (published 7th of April 2014, ~19:00 UTC)
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2076225

本件についてご質問等ございましたら、弊社サポートセンターまでご連絡ください。

◆本件に関するお問い合わせ

日本ストラタステクノロジー株式会社
カスタマーサービス本部 TEL:03-3234-5530

以上