2014 年 6 月 18 日
2014 年 9 月 24 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 "CCS Injection 脆弱性" CVE-2014-0224 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脆弱性が見つかりました。この問題は CVE-2014-0224 として報告されており、「CCS Injection脆弱性」問題とも呼ばれています。このアラート（アラート番号2976）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が稼働するftServerシステムで、OpenSSLパッケージがopenssl-1.0.1e、openssl-0.9.8eおよびopenssl-1.0.0の場合、この問題の影響を受けます。
- Red Hat Enterprise Linux5が稼働するftServerシステムで、OpenSSLパッケージがopenssl-0.9.8eおよびopenssl-1.0.0の場合、この問題の影響を受けます。
- RedHat Enterprise Linux 4が稼働するftServerシステムで、OpenSSLパッケージがopenssl-0.9.7aの場合この問題の影響を受けます。

VMwareシステム

① 影響を受けるESXホストについて

影響が発生するESXホストは下表1の通りです。表1内にはESXホストに対応するAutomated Uptime Layer（以下AUL）の版数も記載しております。

表1 ESXとAULのリリース対応表

VMware ESX	ESX 4.0	ESXi 5.0	ESXi 5.1	ESXi 5.5
AUL	2.0.x / 3.x	4.0.x	4.1.x / 5.0.x	5.1.x

② 影響を受けるftServer管理用仮想マシン（以下ftSys管理アプライアンス）

AUL 4.x、5.0.x 及び 5.1.0に搭載しているftSys管理アプライアンスがこの問題の影響を受けます。

尚、仮想マシンがOpenSSLを使用している場合には、影響を受ける場合があります。

VOSシステム

- OpenSSLを購入され、それがインストールされている全てのVOSシステムではこの問題の影響を受けます。

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、この問題の影響はありません。

everRun及びAvanceシステム

- Avance, everRun MX, everRun Enterprise ではこの問題の影響を受けます。

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はこの問題の影響はありません。

問題の要旨：

本脆弱性が発覚する前のOpenSSLリリースではChageCipherSpecメッセージを適切に制限して処理しないため、OpenSSL間の通信においてゼロレングスのマスターキーの使用をきっかけとして悪意を持った第三者が、TLSハンドシェークを悪用して、セッションの横取りや、重要な情報を取得します。

２．対応方法

ご使用中のOpenSSLのバージョンを確認し、該当する場合には、影響のないOpenSSLコンポーネントバージョンへのアップグレードを推奨します。この問題とOpenSSLバージョンの関連性は以下の通りです。

＊OpenSSL 1.0.1 から 1.0.1g ：影響あり
＊OpenSSL 1.0.1h ：影響なし
＊OpenSSL 1.0.0 から 1.0.0l ：影響あり
＊OpenSSL 1.0.0m ：影響なし
＊OpenSSL 0.9.8za未満 ：影響あり
＊OpenSSL 0.9.8za ：影響なし

Red Hat Enterprise Linux システム

バージョンの確認方法は以下です。
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、RedHatが本問題を修正するパッチを確認し、適切なバージョンへのアップグレードを推奨します。尚、本問題修正のためのアップグレードはOpenSSLライブラリに関係する全てのサービスを再起動するか、システムを再起動する必要があります。

VMwareシステム

① ESXホストの対応について

ESXi5.xについては、VMware社より以下URLにてパッチ情報が公開されております。本問題を修正するパッチをご確認いただき、適切なバージョンへのアップグレードを推奨します。

http://www.vmware.com/security/advisories/VMSA-2014-0006.html

尚、VMware修正パッチを適用するには、AULを以下のリリース以上にバージョンアップする必要があります。

AUL 4.0.3.0（ビルド番号 4.0.3-229）- ESXi 5.0のftServer2600/4500/63x0を使用の場合
AUL 4.1.2.0（ビルド番号 4.1.2-92） - ESXi 5.1のftServer2600/4500/63x0を使用の場合
AUL 5.0.2.0（ビルド番号 5.0.2-233）- ESXi 5.1のftServer2700/4700/6400を使用の場合
AUL 5.1.1.0（ビルド番号 5.1.1-228）- ESXi 5.5のftServer27x0/47x0/64x0を使用の場合

AULのリリースを確認するには、管理アプライアンスにログインして以下のコマンドでビルド番号を確認します。

（実行例）

```
#/opt/ft/bin/ftsmaint -v
ftsys-ftsmaint version 5.0.2-233
```

ESX４がインストールされているシステムにつきましては、VMware社にてESX4のGeneral Supportが2014/5/21で終了している為、本問題に対する修正パッチは作成されません。

但し、信頼出来ないネットワークとの通信を控える事で、本問題の影響を回避可能です。

② ftSys管理アプライアンスの対応について

ftSys管理アプライアンスの修正対応は下表２のとおりです。

表2 ftSys管理アプライアンスの修正対応表

AUL	対応状況	リリース日
4.0.3.2	修正済み	９月 20 日
4.1.2.1	修正済み	９月 11 日
5.0.2.1	修正済み	９月８日
5.1.1.0	修正済み	７月２日

尚、仮想マシン（Windows等）にOpenSSLソフトウェアを導入されている場合には、OpenSSLソフトウェアを修正バージョンに更新してください。

VOSシステム

この問題に対しては不具合 ssl-465 が登録され、V シリーズにおいては、Internet SecurityPack リリース 2.1.1f にて修正版が６月 17 日にリリースされております。本修正には、CVE-2014-0244 を含む最新のセキュリティーパッチが含まれており、その適用には Internet Security Pack のリリースアップが必要となります。

Continuum につきましては、OpebSSL リリース 1.1.1c にて修正版が６月 19 日にリリースされました。

Windowsシステム

OpenSSLが使用されている場合のバージョン確認方法は以下です。
[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。

everRun及びAvanceシステム

everRun Enterpriseでは、CVE-2014-0244を含むRPMを不具合番号bz26709の修正として、everRun Enterpriseリリース7.1.1.1にてリリース致しました。

またeverRun MXについては2014年11月頃に修正版をリリース予定です。

Avanceについては、CVE-2014-0244を不具合番号case#21917として登録修正し、リリース4.0.0.8にて８月１９日にリリース致しました。

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。

- ✧ https://rhn.redhat.com/errata/RHSA-2014-0625.html
- ✧ https://access.redhat.com/security/cve/CVE-2014-0224

VMware ESX上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://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2079783
- ✧ http://www.stratus.com/Services/CustomerSupport/StratusServerSupportDocuments/OSUpdateReleasePolicy/OSReleaseInfoForStratusServer/ESXPatchQualification

関連ドキュメントURL：

CVE-2014-0224についての関連情報は以下をご参照下さい。

- ✧ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224
- ✧ http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
- ✧ http://www.openssl.org/news/secadv_20140605.txt (発行日 5th of June 2014)
- ✧ https://rhn.redhat.com/errata/RHSA-2014-0625.html
- ✧ http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2079783
- ✧ http://www.vmware.com/security/advisories/VMSA-2014-0006.html

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

本文書の改訂履歴

版数	発行日	改訂履歴
第１版	2014 年６月 18 日	初版発行
第２版	2014 年８月７日	１．ご案内の章に everRun/Avance システムの影響度を記載 ２．対応方法の章に VMware システム、VOS システムおよび everRun/Avance システムの修正版の記載を改訂
第３版	2014 年９月２４日	VMware システムおよび Avance システムの修正版の記載を改訂

以上