更新 ： 2014 年 4 月 28 日
作成 ： 2014 年 4 月 17 日
株式会社ネットワールド
ネットワークソリューショングループ

Open SSL の脆弱性について(CVE-2014-0160)

F5 Networks 社製品に含まれる Open SSL に情報漏洩の脆弱性が存在しますのでご連絡いたします。

【1】概要

Open SSL Project が提供する Open SSL(1.0.1 から 1.0.1f)には情報漏えいの脆弱性があります。遠隔の第三者は、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、秘密鍵などの秘匿すべき情報を取得する可能性があります。

【2】詳細

F5 Networks 社より、本脆弱性についての情報が提供されておりますので以下ご参照ください。
(WEB サイト 日本語) http://buzz.f5.com/653SMC7830009g900dPAV00
(ドキュメント 日本語) http://buzz.f5.com/653SMC7830009ga00dPAV00
(WEB サイト 英語) http://support.f5.com/kb/en-us/solutions/public/15000/100/sol15159.html

【3】対象

F5 Networks 社製品においての本脆弱性対象バージョン表

対象製品	本脆弱性が含まれるバージョン	本脆弱性の対象外バージョン
BIG-IP LTM	v11.5.0 – v11.5.1	v11.5.1 HF1– HF2 v11.5.0 HF2– HF3 v11.0.0 – v11.4.1 v10.0.0 – v10.2.4
BIG-IP AAM	v11.5.0 – v11.5.1	v11.5.1 HF1– HF2 v11.5.0 HF2– HF3 v11.4.0 – v11.4.1
BIG-IP AFM	v11.5.0 – v11.5.1	v11.5.1 HF1– HF2 v11.5.0 HF2– HF3 v11.3.0 – v11.4.1
BIG-IP Analytics	v11.5.0 – v11.5.1	v11.5.1 HF1– HF2 v11.5.0 HF2– HF3 v11.0.0 – v11.4.1
BIG-IP APM	v11.5.0 – v11.5.1	v11.5.1 HF1– HF2 v11.5.0 HF2– HF3 v11.0.0 – v11.4.1 v10.1.0 – v10.2.4
BIG-IP ASM	v11.5.0 – v11.5.1	v11.5.1 HF1– HF2 v11.5.0 HF2– HF3 v11.0.0 – v11.4.1 v10.0.0 – v10.2.4
BIG-IP Edge Gateway	None	v11.0.0 – v11.3.0 v10.1.0 – v10.2.4

対象製品	本脆弱性が含まれる バージョン	本脆弱性の対象外 バージョン
BIG-IP GTM	v11.5.0 – v11.5.1	v11.5.1 HF1– HF2 v11.5.0 HF2– HF3 v11.0.0 – v11.4.1 v10.0.0 – v10.2.4
BIG-IP Link Controller	v11.5.0 – v11.5.1	v11.5.1 HF1– HF2 v11.5.0 HF2– HF3 v11.0.0 – v11.4.1 v10.0.0 – v10.2.4
BIG-IP PEM	v11.5.0 – v11.5.1	v11.3.0 – v11.4.1
BIG-IP PSM	None	v11.0.0 – v11.4.1 v10.0.0 – v10.2.4
BIG-IP Web Accelerator	None	v11.0.0 – v11.3.0 v10.0.0 – v10.2.4
BIG-IP WOM	None	v11.0.0 – v11.3.0 v10.0.0 – v10.2.4
ARX	None	v6.0.0 – v6.4.0
Enterprise Manager	None	v3.0.0 – v3.1.1 v2.1.0 – v2.3.0
Fire Pass	None	v7.0.0 v6.0.0 – v6.1.0
BIG-IQ Cloud	None	v4.0.0 – v4.3.0
BIG-IQ Device	None	v4.2.0 – v4.3.0
BIG-IQ Security	None	v4.0.0 – v4.3.0
BIG-IP Edge Clients for Android	None	v2.0.3 – v2.0.4
BIG-IP Edge Clients for Apple iOS	v2.0.0 – v2.0.1 v1.0.5 – v1.0.6	v2.0.2 v1.0.0 – v1.0.4
BIG-IP Edge Clients for Linux	7080.* – 7080.2014.408.* 7090.* – 7090.2014.407.* 7091.* – 7091.2014.408.* 7100.* – 7100.2014.408.* 7101.* – 7101.2014.407.*	6035 – 7071 7080.2014.409.* 7090.2014.408.* 7091.2014.409.* 7100.2014.409.* (11.5.0 HF3) 7101.2014.408.* (11.5.1 HF2)
BIG-IP Edge Clients for MAC OS X	7080.* – 7080.2014.408.* 7090.* – 7090.2014.407.* 7091.* – 7091.2014.408.* 7100.* – 7100.2014.408.* 7101.* – 7101.2014.407.*	6035 – 7071 7080.2014.409.* 7090.2014.408.* 7091.2014.409.* 7100.2014.409.* (11.5.0 HF3) 7101.2014.408.* (11.5.1 HF2)
BIG-IP Edge Clients for Windows	7080.* – 7080.2014.408.* 7090.* – 7090.2014.407.* 7091.* – 7091.2014.408.* 7100.* – 7100.2014.408.* 7101.* – 7101.2014.407.*	6035 – 7071 7080.2014.409.* 7090.2014.408.* 7091.2014.409.* 7100.2014.409.* (11.5.0 HF3) 7101.2014.408.* (11.5.1 HF2)

【4】影響

BIG-IP 製品群に関しては、一部を除き影響を受けません（ハードウェア/VE プラットフォーム共通）

-TMOS v11.5.0、11.5.1 以外の OS をご利用のお客様は本脆弱性の影響はありません

-TMOS v11.5.0、11.5.1 で NATIVE モードの SSL Cipher をご利用のお客様は本脆弱性の影響を受けません

影響を受けるケース

-TMOS v11.5.0 あるいは v11.5.1 且つ 、COMPAT モードの SSL Cipher をご利用のお客様

-TMOS v11.5.0 あるいは v11.5.1 の設定用 Web 管理画面へのアクセス（Management ポート、および Self-IP）

Edge Client に関しては、一部影響を受ける Open SSL バージョンを使用しております

-Edge Client for Android は影響を受けません

影響を受けるケース

-Edge Client for Windows, Mac OS, Linux, iOS の特定のバージョンかつ、

-本脆弱性のある BIG-IP 製品（APM）への接続時

-悪意のある APM、シミュレートされた APM への接続時

【5】対策

1. 本脆弱性対象外バージョンへのアップグレードを行ってください。

F5 ダウンロードサイト（https://downloads.f5.com/esd/index.jsp)より、イメージファイルのダウンロードが行えます。

「Find a Download」 => 「BIG-IP v11.x / Virtual Edition」 => プルダウンメニューより v11.5.0 または v11.5.1 を選択します。ダウンロード画面が表示されますので、以下の Hot Fix をダウンロードください。

TMOS v11.5.0 ご利用の場合　Hotfix-BIGIP-11.5.0.3.0.236-HF3　をダウンロードください
TMOS v11.5.1 ご利用の場合　Hotfix-BIGIP-11.5.1.2.0.121-HF2　をダウンロードください

2. 本脆弱性対象バージョンでも、SSL の Cipher に NATIVE を利用することで対策が可能です。

※SSL の設定には、NATIVE と COMPAT の 2 つの処理モードが存在します。**BIG-IP のデフォルトの設定では NATIVE モードに設定されていますので、変更しない限り、本脆弱性の対象となりません。**

-NATIVE とは F5 独自のトラフィック管理 OS（TMOS）上に実装された SSL 処理モードです。

-COMPAT とは Open SSL ライブラリを使用する SSL 処理モードです

3. Web 管理用の Management IP や Self-IP アクセスをインターネットに公開させないでください。

インターネット経由で Web 管理へアクセスする必要がある場合、下記の対応で緩和できます。

-tmsh 接続のみアクセス制限を行う。

以上

※参考情報

・The Heartbleed Bug
http://heartbleed.com/

・BIG-IP third-party software matrix
(v11.x) http://support.f5.com/kb/en-us/solutions/public/14000/400/sol14457.html
(v9.x-10.x) http://support.f5.com/kb/en-us/solutions/public/9000/400/sol9445.html