BIG-IP 管理 GUI Apache 脆弱性対策手順書

（Ver9.1.x、Ver9.3.1）

株式会社日立製作所

目次

商標名称について

本書で使用されている登録商標は以下の通りです。

・Apache、Tomcat、Apache James、Luceneは、Apache Software Foundationの登録商標または商標です。

・Apache、Tomcatは、Apache Software Foundationの登録商標または商標です。

・BIG-IPは、F5 Networks, Inc の商標、または登録商標です。

・UNIXは、The Open Group の登録商標です。

・Windows® の正式名称はMicrosoft® Windows® Operating Systemです。

・Windowsは、米国Microsoft Corporation.の米国およびその他の国における登録商標です。

・Tera Term、Tera Term Pro は寺西 高氏が著作権を所有するフリーソフトウェアです。

・PuTTYは、Simon Tatham氏が開発・公開しているターミナルエミュレータです。

その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

はじめに

BIG-IPの管理GUI機能を提供するApache HTTP ServerにRangeヘッダに多数のRangeを表記することで、リモートからのDoSアタックの影響を受ける脆弱性（CVE-2011-3192）が判明しました。
一般的には"Apache Killer"と呼ばれるこの脆弱性の攻撃により、httpdのプロセスは利用可能なCPUリソースをすべて消費します。
CPUリソースの枯渇により、管理GUI、SSHセッション、および他のプロセスの応答が非常に遅いか、場合によっては完全に応答しなくなる可能性があります。
本脆弱性への攻撃により、TMM などの処理を行っている Host 部の応答時間が遅れる・もしくは無応答になることで、Watchdog 機能による Reboot が引き起こされる可能性があります。
この脆弱性に対応するため管理 GUI 宛への通信から“Range”と“Request-Range”ヘッダを受け付けなくするには本書の手順を実施します。

なお、上位の Firewall の設定や、BIG-IP の PortLockdown の設定にて、不特定のユーザーが BIG-IP の管理 GUI に HTTPS でアクセスできない環境である場合は、脆弱性は存在してもその脆弱性による影響は希薄と判断されます。

前提知識

本作業を行うにあたり、以下の知識が必要になります。

- 簡単なBIG-IPの操作ができること。
  （BIG-IPへSSH及びコンソールでの接続、ファイル編集及び、デーモン再起動等）
- 基本的なUnixコマンド操作が出来ること。
  （ファイルのコピー、移動、viエディタによるファイル編集など)
- BIG-IPのUCSファイルについて理解していること。
  （UCSファイルに含まれる設定ファイルなどを理解していること。）

※ご案内するファイルは全て重要なファイルですので、修正前には必ずバックアップファイルを採取いただくと共に、編集の際、留意してご対応下さい。

対象形名

以下に示すBIG-IP1500 全形名
GV0LB150-10NNN0, GV0LB150-20NNNN0, GV0LB151-10NNNN1, GV0LB151-20NNNN1

（注）本書に記載の製品の仕様は、製品の改良などのため予告なく変更することがあります。

管理 GUI　Apache 脆弱性対策手順

1　SSH もしくはコンソールからのアクセス

Apache 脆弱性対策手順を行うには、コンソールもしくは SSH 経由で BIG-IP の CLI にアクセスし実施する必要があります。

本手順書記載の作業は Windows 標準搭載のハイパーターミナルで行えます。ハイパーターミナルの代わりに Tera Term を利用することも可能です。Tera Term を利用する場合の設定は 1-1（４）に準じて行ってください。ここではハイパーターミナルの接続例を示します。SSH を利用する場合は 1-1 の手順を付録と読み替えてください。1-2 以降の手順はハイパーターミナル使用時、SSH 使用時ともに同じです。

1-1 コンソール接続の方法

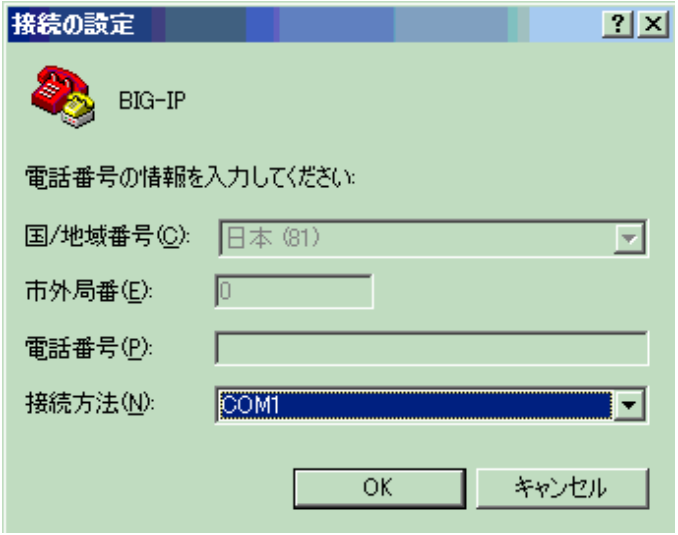
（１）ハイパーターミナルの接続・起動

設定用 PC で Windows 標準搭載のハイパーターミナルを起動します。ハイパーターミナルの起動方法は搭載する Windows により異なります。

（２）名前の入力

ハイパーターミナルを起動すると【接続の設定画面】が表示されますので、任意の“名前”を入力します。

（３）接続先 RS-232C ポートを指定します。



（4）各種設定

“ ビット/秒 ” を “ 19200 ”、“ フロー制御 ” をなしに変更し、[OK]ボタンをクリックします。

Tera Term の場合は上の Setup をクリックして、Serial port を選択。

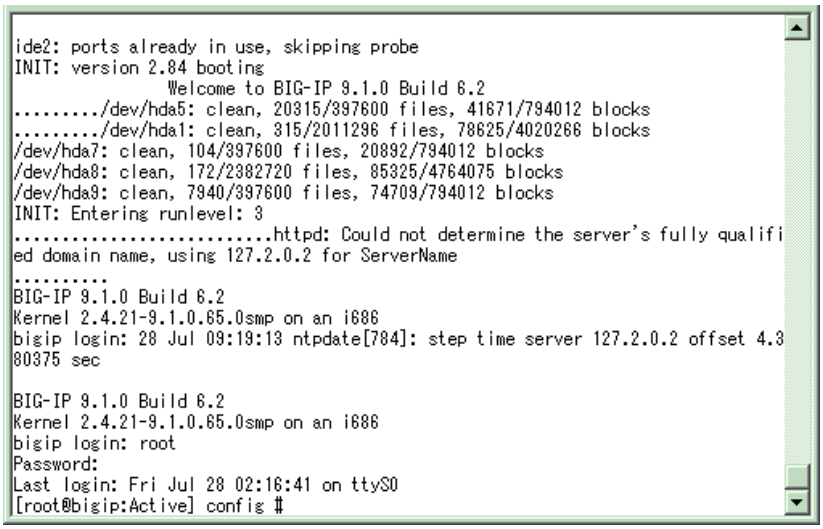
“ Baud rate ” を “ 19200 ”、“ Data ” を “ 8bit ”、“ Stop ” を “ 1bit ”、他を “ none ” に選択し、[OK]ボタンをクリックします。

1-2 BIG-IP ログイン

BIG-IP へのログイン

（Enter）キーを押すと　login：　プロンプトが表示されますので root と入力します。

続いて　Password：　には設定されているパスワードを入力しログインします。



2 httpd.conf ファイルのバックアップ

次項で編集するhttpd.confファイルのバックアップを作成します。

#cp –p /config/httpd/conf/httpd.conf /config/httpd/conf/httpd.conf.org

3 ファイルの編集(httpd.conf)

vi コマンドで httpd.conf を編集します。

#vi /config/httpd/conf/httpd.conf

下記「追加文字列」の赤字部分の 3 行を httpd.conf の最終行に追記し保存してください。

追加文字列
～最終行に追加～ **# CVE-2011-3192** **RequestHeader unset Range** **RequestHeader unset Request-Range**

4 httpd デーモンの再起動

次のコマンドでhttpdを再起動します。

#bigstart restart httpd

(正常例)

```
# bigstart restart httpd
stopping httpd:[OK]
starting  httpd:[OK]
```

5 管理 GUI へのアクセス確認

管理GUIへアクセスし、ログインできることを確認してください。

6 編集前のファイルへの戻し方法

編集を行った後、問題が発生した場合は下記のコマンドでバックアップからhttpd.confを回復し、httpデーモンを再起動してください。

（注）5 項で管理 GUI アクセスに異常が発生した場合のみ実行

```
#cp –p /config/httpd/conf/httpd.conf.org /config/httpd/conf/httpd.conf
# bigstart restart httpd
```

7 UCS ファイル反映手順

上記で編集したhttp.conf ファイルはUCSファイルにバックアップされないため、以下の手順でUCSのバックアップ対象となるように設定します。

7-1 cs.dat ファイルのバックアップ

ファイルを編集する前にバックアップを作成します。

（例）#cp -p /usr/libdata/configsync/cs.dat /usr/libdata/configsync/cs.dat.org

7-2 ファイルの編集(cs.dat)

v9.3.xではcs.datのアクセス権がReadOnlyに設定されているため、以下のようにパーミッションを変更します。v9.1.xではアクセス権がRead/Writeのためパーミッション変更は不要です。

 # chmod 755 /usr/libdata/configsync/cs.dat

/usr/libdata/configsync/cs.dat ファイルの"config directory"内を以下のように編集します。save.の後の数値は4800番台で使われていない数値を使用して下さい。

※ 編集する箇所や追加行は赤字にしております。

下記が /usr/libdata/configsync/cs.datファイル編集内容です。

変更前	変更後
~ 前略 ~	~ 前略 ~
【 config directory 】	【 config directory 】
save.2200.ignore = (/config/httpd/conf/ssl.crt/.*)	save.2200.ignore = (/config/httpd/conf/ssl.crt/.*)
save.2210.ignore = (/config/httpd/conf/ssl.key/.*)	save.2210.ignore = (/config/httpd/conf/ssl.key/.*)
save.2220.ignore = /config/httpd/conf/httpd.conf	#save.2220.ignore = /config/httpd/conf/httpd.conf
save.2221.ignore = /config/httpd/conf.d/ssl.conf	save.2221.ignore = /config/httpd/conf.d/ssl.conf
save.2222.ignore = (/config/ssl/ssl.key/.*)	save.2222.ignore = (/config/ssl/ssl.key/.*)
save.2230.save_pre = cert_save_pre	save.2230.save_pre = cert_save_pre
	~ 中略 ~
~ 以降略 ~	save.4700.file = /root/.bash_profile
	save.4710.file = /root/.bashrc
	save.4800.dir = /home
	# 'UCS save' operations
	save.4851.file = /usr/libdata/configsync/cs.dat
	save.4851.local = yes
	save.4853.file = /config/httpd/conf/httpd.conf
	save.4853.local = yes
	~ 以降略 ~

行頭に“＃”を追加する。

Save.4800.dir = /home の行の後に追加する。既に追加されている場合は追加不要です。

7-3 UCS ファイルの作成

次の方法でUCSファイルを作成します。
管理GUIより、System->Archiveに進み、Createボタンをクリックして作成します。

7-4 UCS ファイルの解凍

UCSファイルは管理GUIで作成後、ローカルPC上にダウンロードして正常に解凍できるか確認して下さい。
このファイル（拡張子ucs）は、TAR-GZ形式で各種設定ファイルを圧縮したものになります。
　　一般的な解凍ツールで内容を確認できます。

7-5 編集ファイルの確認

UCSを解凍した場合の次のパスに編集したファイルが格納されている事を確認してください。

/usr/libdata/configsync/cs.dat.[Host名]_cs

/config/httpd/conf/httpd.conf.[Host 名]_cs

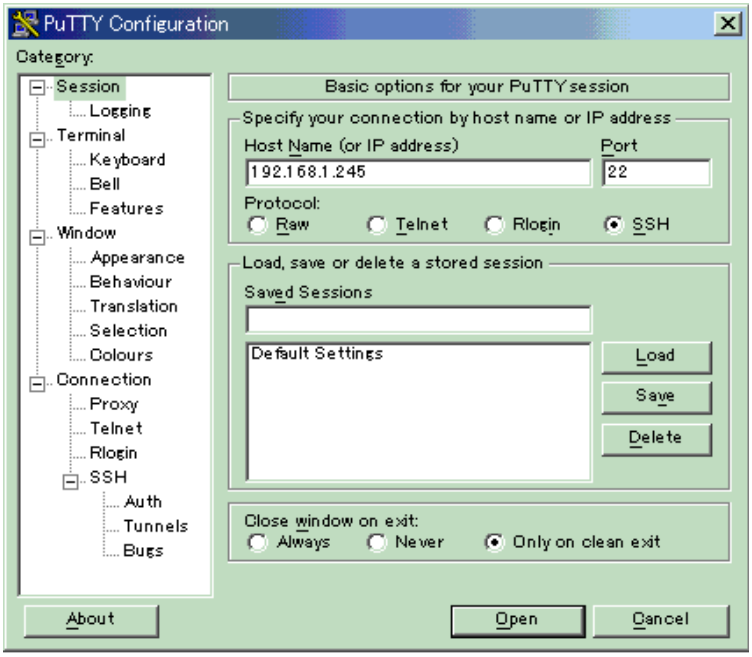
― 以上 ―

＜付録１　シリアルケーブルを準備できない場合の代替手段＞

シリアルケーブルを準備できない場合、コンソール用のソフトウェアとしてハイパーターミナルの代わりに SSH クライアントを利用することができます。SSH クライアントは PuTTY 等のフリーソフトウェアを利用できますのでインターネットからダウンロードしてインストールしてください。ここでは PuTTY を利用する接続手順について説明します。

（１）PuTTY を起動する。

PuTTY.exe をダブルクリック以下の画面が表示されます。Host Name として BIG-IP の IP アドレスである 192.168.1.245 を入力して Open ボタンを押します。

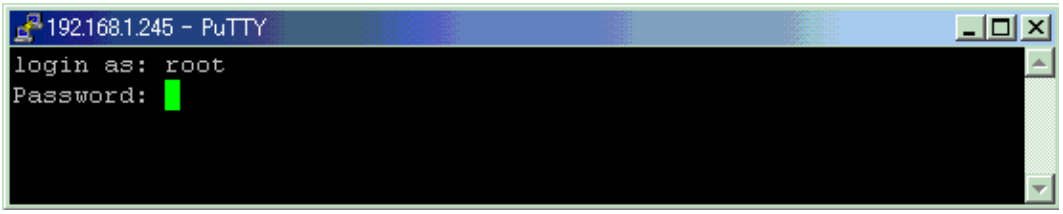


（２）BIG-IP のコンソールにログインする。

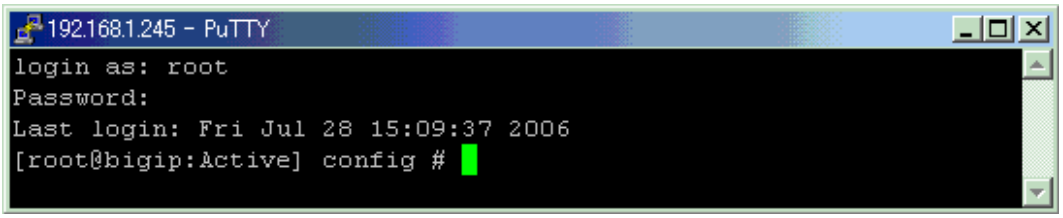
Login as ：　の表示で　root　と入力します。

次に Password ：　の表示で　default　と入力します。

ログイン画面



ログイン後の画面



作業手順は、ハイパーターミナルを利用した場合（「2 httpd.conf ファイルのバックアップ」以降）と同じです。