

README

hashdos-workaround-js4.jar

本書は、Interstage Application Server/Interstage Web Server (以降Interstage Application ServerまたはInterstageと表記します)の回避モジュール(hashdos-workaround-js4.jar)の適用方法について記したものです。本文中の記載内容は予告なしに変更される場合があります。

■商標について

- OracleとJavaは、Oracle Corporationおよびその子会社、関連会社の米国およびその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。
- Microsoft、Windows、Windows Server、Windows Vista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。
- Red Hatは、米国およびその他の国におけるRed Hat, Inc. の登録商標です。
- Linuxは、Linus Torvalds氏の米国およびその他の国における登録商標あるいは商標です。
- その他の会社名および製品名は、それぞれの会社の登録商標もしくは商標です。

■表記について

本書では、プラットフォームごとに内容が異なる箇所にはプラットフォームを示すマークを付けて記載しています。

	Windows NT Server 4.0/ Windows 2000 Server/ Windows Server 2003/ Windows Server 2003 R2/ Windows Server 2008/ Windows Server 2008 R2/ Windows XP/ Windows Vista/ Windows 7
	Oracle Solaris 7/ Oracle Solaris 8/ Oracle Solaris 9/ Oracle Solaris 10
	RHEL-AS2.1 (x86)/ES2.1 (x86)/ RHEL-AS3 (x86)/ES3 (x86)/ RHEL-AS4 (IPF)/ RHEL-AS4 (x86)/AS4 (EM64T)/ RHEL5 (IPF)/ RHEL5 (x86)/ RHEL5 (Intel64)/ RHEL6 (x86)/ RHEL6 (Intel64)

Copyright 2012 FUJITSU LIMITED

1. 回避モジュール(hashdos-workaround-js4.jar)について

本回避モジュールは、CVE-2011-4858、CVE-2011-5035として公開されたサービス運用妨害(DoS)となる脆弱性を回避するためのモジュールです。SEC-1767(社内管理番号)に対応しています。

この脆弱性は、リモートの攻撃者から、同一のハッシュ値となるように、Servletサービス/Java EEのWebコンテナへ細工されたリクエストが送信されることにより、Webサーバ上のCPUを大量に消費し、サービス運用妨害(DoS)となる可能性があるというものです。

本回避モジュールを適用すると、Servletコンテナが受け付けるHTTPリクエストボディサイズの最大値を10240バイトに制限できるため、当該脆弱性の影響を十分に軽くできます。HTTPリクエストボディサイズの最大値は変更可能です。ユーザアプリケーションとして考えられるPOSTリクエストの最大値を設定してください。Interstage Application Serverでは10KBを推奨します。

■提供情報

README.pdf : 適用方法の説明(本書)

hashdos-workaround-js4.jar : 回避モジュール(Tomcat4.1ベースのServletサービス用)

2. 該当製品

該当製品については、以下のサイトで確認してください。

[Interstage Application Server：サービス運用妨害\(DoS\)となる脆弱性 \(CVE-2011-4858, CVE-2011-5035\)](#)

本回避モジュールは、Tomcat4.1ベースのServletサービス用のモジュールです。パッケージ名が「F3FMjs4」または「FJSVjs4」の製品が該当します。

3. 適用方法

回避モジュールを適用するには、以下の手順で操作します。

1. Interstage、IJServerワークユニット、Interstage管理コンソール、Webサーバを停止します。

Windows[®]2/64

- 1) Interstage、IJServerワークユニットを停止します。
 - V6/V7で、Interstage Application Server Web-J Editionの場合
isstopwuコマンドで、すべてのIJServerワークユニットを停止します。
 - V6/V7で、Interstage Application Server Web-J Edition以外の場合
isstopコマンドにオプション“-f”を指定して実行し、Interstageを停止します。
 - V8以降の場合
isstop -f -sコマンド(全強制停止モード)を使用して、Interstageを停止します。
- 2) Interstage管理コンソール、Webサーバを停止します。
Windowsの[管理ツール] > [サービス]で、以下のサービスを停止します。
 - Interstage Operation Tool
 - Interstage Operation Tool (FJapache)
 - Interstage JServlet (OperationManagement)
 - FJapache [Interstage HTTP Serverを使用している場合]
 - Interstage HTTP Server (Webサーバ名)
[V9以降で、Interstage HTTP Serverの複数Webサーバを使用している場合]
 - World Wide Web Publishing Service [V7以降でInternet Information Servicesを使用している場合]

Solaris

- 1) スーパーユーザになります。
 - 2) shutdownコマンドを実行して、OpenBoot環境に入ります。
例)

```
/usr/sbin/shutdown -y -g0 -i0
```
 - 3) システムをシングルユーザモードで起動します。
例)

```
boot -s
```
 - 4) 以下のようなメッセージが表示されたら、<password>にスーパーユーザのパスワードを入力します。

```
INIT: SINGLE USER MODE
Type Ctrl-d to proceed with normal startup,
(or give root password for system maintenance): <password> <Return>
```
 - 5) mountallコマンドを実行して、必要なファイルシステムをマウントします。
例)
-

```
/usr/sbin/mountall -l
```

Linux32/64

- 1) shutdownコマンドを実行して、シングルユーザモードに切り替えます。

例)

```
/sbin/shutdown now
```

- 2) mountコマンドを実行して、必要なファイルシステムをマウントします。

例)

```
/bin/mount -a
```

2. 回避モジュールを適用します。

- 1) 以下のディレクトリに移動します(パスはフルパスで指定)。

Windows32/64 例) インストールディレクトリが「C:\¥Interstage」の場合

```
cd C:\¥Interstage¥F3FMjs4¥server¥classes
```

Solaris Linux32/64 例) インストールディレクトリが「/opt」の場合

```
cd /opt/FJSVjs4/server/classes
```

- 2) 回避モジュールを適用します。

Windows32/64 例) JDK1.3の場合

```
C:\¥Interstage¥jdk13¥bin¥jar xf [任意のディレクトリ]¥hashdos-workaround-js4.jar
```

Solaris Linux32/64 例) JDK1.3の場合

```
/opt/FJSVawjbk/jdk13/bin/jar xf [任意のディレクトリ]/hashdos-workaround-js4.jar
```

V7以降の場合は、3)、4)の手順も実施してください。

- 3) 以下のディレクトリに移動します(パスはフルパスで指定)。

Windows32/64 例) インストールディレクトリが「C:\¥Interstage」の場合

```
cd C:\¥Interstage¥F3FMjs4¥server6¥classes
```

Solaris Linux32/64 例) インストールディレクトリが「/opt」の場合

```
cd /opt/FJSVjs4/server6/classes
```

- 4) 回避モジュールを適用します。

Windows32/64 例) JDK1.3の場合

```
C:\¥Interstage¥jdk13¥bin¥jar xf [任意のディレクトリ]¥hashdos-workaround-js4.jar
```

Solaris Linux32/64 例) JDK1.3の場合

```
/opt/FJSVawjbk/jdk13/bin/jar xf [任意のディレクトリ]/hashdos-workaround-js4.jar
```

3. Solaris Linux32/64 回避モジュールの属性を以下のように設定します。

directory or file	owner	group	permission
org	root	sys	755
org/apache	root	sys	755
org/apache/catalina	root	sys	755
org/apache/catalina/core	root	sys	755
org/apache/catalina/core/StandardEngineValve.class	root	sys	444

例)

```
chown -R root:sys org
chmod -R 755 org
chmod 444 org/apache/catalina/core/StandardEngineValve.class
```

-
4. **Solaris** **Linux32/64** 回避モジュールが正しく格納されたこと、手順3. で設定した属性が正しいことを確認します。

例) インストールディレクトリが「/opt」の場合

```
ls -lR /opt/FJSVjs4/server/classes/org
```

5. Interstage、IJServerワークユニット、Interstage管理コンソール、Webサーバを起動します。

Windows32/64

- 1) Interstage管理コンソール、Webサーバを起動します。
Windowsの[管理ツール] > [サービス]で、以下のサービスを開始します。
 - Interstage Operation Tool
 - Interstage Operation Tool (FJapache)
 - Interstage JServlet (OperationManagement)
 - FJapache [Interstage HTTP Serverを使用している場合]
 - Interstage HTTP Server (Webサーバ名)
[V9以降で、Interstage HTTP Serverの複数Webサーバを使用している場合]
 - World Wide Web Publishing Service [V7以降でInternet Information Servicesを使用している場合]
- 2) Interstage、IJServerワークユニットを起動します。
「運用ガイド」(V8以前)、「運用ガイド(基本編)」(V9以降)を参照して、通常通り起動します。

Solaris

- 1) shutdownコマンドを実行して、マルチユーザモードに戻します。
例)

```
/usr/sbin/shutdown -y -g0 -i6
```

Linux32/64

- 1) shutdownコマンドを実行して、マルチユーザモードに戻します。
例)

```
/sbin/shutdown -r now
```

4. 定義の変更方法

Servletコンテナが受け付けるHTTPリクエストボディサイズの最大値を、デフォルト(10240バイト)から変更できます。必要に応じて、定義を変更してください。

定義名 : `com.fujitsu.interstage.servlet.request.maxContentLength`

定義はIJServerワークユニットごとの設定になっているため、変更が必要なIJServerワークユニットの数分、定義を変更する必要があります。定義を変更するには、Interstage管理コンソールまたはisj2eedadminコマンド(V8以降)を使用します。ここでは、Interstage管理コンソールを使った変更方法を説明します。

操作手順

- 1) Interstage管理コンソールを起動します。
 - 2) [Interstage Application Server] (注) > [システム] > [ワークユニット] > [IJServer名]を選択して[操作]タブに移動します。
注) V7以降
 - 3) [停止]ボタンでIJServerワークユニットを停止します。
 - 4) [環境設定]タブに移動します。
 - 5) [ワークユニット設定]の[表示]をクリックします。
-

- 6) [Java VMオプション]に以下の形式でHTTPリクエストボディサイズの最大値を指定し、[適用]ボタン(V7以前の場合は[更新]ボタン)をクリックします。

```
-Dcom.fujitsu.interstage.servlet.request.maxContentLength=最大値
```

- 最大値は、1~2147483647バイトで指定します。
 - 0以下を指定すると、「制限なし」になります。
 - デフォルトは10240バイトです。
- 7) [操作]タブに移動します。
- 8) [起動]ボタンでIJServerワークユニットを起動します。

5. 復元方法

適用した回避モジュールを削除して、適用前の状態に復元するには、以下の手順で操作します。

1. Interstage、IJServerワークユニット、Interstage管理コンソール、Webサーバを停止します。

停止方法は、「3. 適用方法」の手順1.を参照してください。

2. 回避モジュールを削除します。

- 1) 以下のディレクトリに移動します(パスはフルパスで指定)。

Windows32/64 例) インストールディレクトリが「C:\¥Interstage」の場合

```
cd C:\¥Interstage¥F3FMjs4¥server¥classes
```

Solaris **Linux32/64** 例) インストールディレクトリが「/opt」の場合

```
cd /opt/FJSVjs4/server/classes
```

- 2) 回避モジュール(orgディレクトリ配下のすべてのファイル)を削除します。誤って他のディレクトリを削除しないように、十分注意してください。

Windows32/64

```
rmdir /S org
```

Solaris **Linux32/64**

```
rm -ri org
```

V7以降の場合は、3)、4)の手順も実施してください。

- 3) 以下のディレクトリに移動します(パスはフルパスで指定)。

Windows32/64 例) インストールディレクトリが「C:\¥Interstage」の場合

```
cd C:\¥Interstage¥F3FMjs4¥server6¥classes
```

Solaris **Linux32/64** 例) インストールディレクトリが「/opt」の場合

```
cd /opt/FJSVjs4/server6/classes
```

- 4) 回避モジュール(orgディレクトリ配下のすべてのファイル)を削除します。

Windows32/64

```
rmdir /S org
```

Solaris **Linux32/64**

```
rm -ri org
```

3. Interstage、IJServerワークユニット、Interstage管理コンソール、Webサーバを起動します。

起動方法は、「3. 適用方法」の手順 5.を参照してください。