

2013 年 9 月 26 日
(改訂日:2013 年 11 月 20 日)
※改訂履歴は最終ページに記載

お客様各位

株式会社 セゾン情報システムズ
HULFT 事業部

HULFT クラウドの脆弱性に関するお知らせ

HULFT クラウドにおいて、セキュリティの脆弱性に関する新たな問題が発見されました。
回避策について下記のとおりご案内申し上げますので、ご確認の上、適用をお願いいたします。

－ 記 －

1. 対象製品

HULFT クラウド Ver. 1.0.0～Ver. 1.4.0A

2. 脆弱性の原因と内容について

HULFT クラウドで使用している Web アプリケーションフレームワーク (Struts Ver. 2.1.8.1～
2.3.15.1) に下記の脆弱性が存在します。

<Struts2 の問題>

- S2-018 - Broken Access Control Vulnerability in Apache Struts2
<http://struts.apache.org/release/2.3.x/docs/s2-018.html>
- S2-019 - Dynamic Method Invocation disabled by default
<http://struts.apache.org/release/2.3.x/docs/s2-019.html>

3. S2-018に対する回避策

Web サーバで下記のプレフィックスを含んだリクエストを拒否する設定を行うことで、脆弱性を防ぐことが可能です。既に設定を行っている場合は必要ありません。

```
action:
redirect:
redirectAction:
```

※Apache2.2での設定例

- (1) mod_rewrite.soモジュールの有効化
httpd.confを編集し、下記行のコメントを外してください。

`LoadModule rewrite_module modules/mod_rewrite.so`
- (2) 脆弱性の原因となるプレフィックスを含んだリクエストの拒否設定
httpd.confに下記の内容を追記します。
“webft”の箇所は実際のコンテキスト名に置き換えてください。

```
<IfModule mod_rewrite.c>

    RewriteEngine On

    RewriteCond %{QUERY_STRING} action:
    RewriteRule ^/webft/.+ - [F]

    RewriteCond %{QUERY_STRING} redirect:
    RewriteRule ^/webft/.+ - [F]

    RewriteCond %{QUERY_STRING} redirectAction:
    RewriteRule ^/webft/.+ - [F]

</IfModule>
```

- (3) Apacheの再起動
Apacheの再起動を行います。

4. S2-019に対する回避策

HULFT クラウドは認証を行っていない HTTP(S) リクエストについては拒否するよう設計されており、サーバプログラムの内部仕様についても非公開となっております。そのため、S2-019 の脆弱性につきましては、攻撃が成立する条件は極めて少ないことを確認しております。しかしながら、安全にお使い頂くために以下の脆弱性の対処を行ってください。

Struts 設定ファイル (struts.xml) の編集を行うことで、脆弱性を防ぐことが可能です。以下の手順に従って脆弱性の対処を Struts 設定ファイル (struts.xml) に適用してください。

手順① (Apache Tomcat)

- (1) Tomcatの停止
HULFT クラウドをデプロイしているTomcatを停止してください。
- (2) HULFT クラウドのバックアップ
HULFT クラウドのバックアップを行ってください。バックアップの方法は、「HULFT クラウド 導入マニュアル」をご参照ください。
- (3) Struts設定ファイル (struts.xml) の編集
以下のフォルダにあるStruts設定ファイル (struts.xml) に編集を加えます。
Tomcatインストールフォルダ¥webapps¥webft¥WEB-INF¥classes

【編集前】
<constant name="struts.enable.DynamicMethodInvocation" value="true"/>

【編集後】
<constant name="struts.enable.DynamicMethodInvocation" value="false"/>
- (4) Tomcatの起動
Tomcatの起動を行います。
- (5) Struts設定ファイル (struts.xml) の編集後の確認
疎通テストを行なって、通常通り動作することをご確認ください。疎通テスト方法は、「HULFT クラウド 導入マニュアル」をご参照ください。

手順② (IBM WebSphere Application Server)

- (1) IBM WebSphere Application Serverの停止
HULFT クラウドをデプロイしているIBM WebSphere Application Serverを停止してください。
- (2) HULFT クラウドのバックアップ
HULFT クラウドのバックアップを行ってください。バックアップの方法は、「HULFT クラウド 導入マニュアル」をご参照ください。
- (3) Struts設定ファイル (struts.xml) の編集
以下のフォルダにあるStruts設定ファイル (struts.xml) に編集を加えます。
WebSphereインストールフォルダ¥サーバ名¥profiles¥プロファイル名¥installedApps¥セル名¥webft.ear¥webft.war¥WEB-INF¥classes

【編集前】
<constant name="struts.enable.DynamicMethodInvocation" value="true"/>

【編集後】
<constant name="struts.enable.DynamicMethodInvocation" value="false"/>
- (4) IBM WebSphere Application Serverの起動
IBM WebSphere Application Serverの起動を行います。
- (5) Struts設定ファイル (struts.xml) の編集後の確認
疎通テストを行なって、通常通り動作することをご確認ください。疎通テスト方法は、「HULFT クラウド 導入マニュアル」をご参照ください。

5. 製品の対応

脆弱性の対処を行った HULFT クラウド (2013 年 12 月リリース予定) をご提供いたします。

以上

【改訂履歴】

2013/11/20 「3. S2-018に対する回避策」 (2) の設定例を、[F] から - [F] へ訂正いたしました。