SoftBank Technology

ソフトバンク・テクノロジー株式会社

脆弱性調査レポート

Apache Struts 2 のマルチパーサー「jakarta」および「jakarta-stream」の脆弱性により、リモートから任意のコードが実行可能な脆弱性(CVE-2017-5638)(S2-046)に関する調査レポート

【概要】

Apache Struts 2 に、リモートより任意のコードが実行可能な脆弱性(CVE-2017-5638)(S2-046)及び、その脆弱性を利用する攻撃コードが発見されました。この脆弱性は、前回公開しましたレポート、「Apache Struts 2 のマルチパーサー「jakarta」の脆弱性により、リモートから任意のコードが実行可能な脆弱性(CVE-2017-5638)(S2-045)に関する調査レポート」の脆弱性に関連しており、「S2-045」と同じ種類の脆弱性が別のパラメータ処理時にも存在しているもので、新たな脆弱性識別子「S2-046」が採番されました。

また本脆弱性は、マルチパーサー「jakarta」のみではなく、「S2-045」の脆弱性情報公開当初、開発元より同脆弱性の対策案としてアナウンスされた、別のマルチパーサーへ切り替える案にて、代替マルチパーサーとして提示されたマルチパーサー「jakarta-stream」を使用している場合にも影響を受けます。

この脆弱性を利用した攻撃が成立した場合、リモートから Apache Struts2 がインストールされた Web アプリケーションサーバーの実行権限で任意のコードを実行される危険性があります。

本レポート作成(2017 年 3 月 28 日)時点において、既に Apache Software Foundation よりこの脆弱性が修正されたバージョンがリリースされております。しかしながら、「S2-045」の対策として、マルチパーサーを「jakarta-stream」に変更する案を採用し、脆弱性が残存している状態で運用されているシステムに対しての注意喚起の意味込めて、今回、この脆弱性(CVE-2017-5638)(S2-046)の再現性について検証を行いました。

なお、「S2-045」の脆弱性対策として、脆弱性が修正されたバージョンへアップグレードした場合には、本脆弱性の影響は受けません。

【影響を受ける可能性があるシステム】

- Apache Struts 2.3.5 から 2.3.31 までのバージョン
- Apache Struts 2.5 から 2.5.10 までのバージョン

【対策案】

本レポート作成(2017 年 3 月 28 日)時点において、Apache Software Foundation より、この脆弱性を修正するバージョンがリリースされています。当該脆弱性が修正されたバージョンへとアップグレードしていただくことを推奨いたします。

ただちにアップグレードすることが困難である場合、本脆弱性を解消したプラグイン「Secure Jakarta Multipart parser plugin」または「Secure Jakarta Stream Multipart parser plugin」を使用することにより、「S2-045」および「S2-046」の問題を回避することが可能です。なお、各プラグインは以下の Apache Struts のバージョンで使用可能です。

「Secure Jakarta Multipart parser plugin」

- Apache Struts 2.3.8 から 2.5.5 までのバージョン

「Secure Jakarta Stream Multipart parser plugin」

- Apache Struts 2.3.20 から 2.5.5 までのバージョン

プラグインの設定手順は以下の通りです。なお、下記は弊社環境(Apache Struts 2.3.31 を使用)の場合での設定例です。詳細は以下の開発元の Web サイトをご確認ください。

GitHub - apache/struts-extras

- 「Secure Jakarta Multipart parser plugin」を使用する場合

1. 開発元より提供されている「Secure Jakarta Multipart parser plugin」のプラグインファイルを/WEB-INF/lib 配下に配置します。

```
[root@localhost ~]# find /var/lib/tomcat/webapps/struts2-showcase/WEB-INF/lib/ -name struts2-secure-jakarta*.jar
/var/lib/tomcat/webapps/struts2-showcase/WEB-INF/lib/struts2-secure-jakarta-multipart-parser-plugin-1.1.jar
```

2. struts.xml に以下の内容を追記します。

```
<bean type="org.apache.struts2.dispatcher.multipart.MultiPartRequest"
      class="org.apache.struts.extras.SecureJakartaMultipartParser"
      name="secure-jakarta"
      scope="default"/>

<constant name="struts.multipart.parser" value="secure-jakarta"/>
```

3. Web アプリケーションサーバーを再起動します。

- 「Secure Jakarta Stream Multipart parser plugin」を使用する場合

1. 開発元より提供されている「Secure Jakarta Stream Multipart parser plugin」のプラグインファイルを/WEB-INF/lib 配下に配置します。

```
[root@localhost ~]# find /var/lib/tomcat/webapps/struts2-showcase/WEB-INF/lib/ -name struts2-secure-jakarta*.jar
/var/lib/tomcat/webapps/struts2-showcase/WEB-INF/lib/struts2-secure-jakarta-stream-multipart-parser-plugin-1.1.jar
```

2. struts.xml に以下の内容を追記します。

```
<bean type="org.apache.struts2.dispatcher.multipart.MultiPartRequest"
      class="org.apache.struts.extras.SecureJakartaStreamMultiPartRequest"
      name="secure-jakarta-stream"
      scope="default"/>

<constant name="struts.multipart.parser" value="secure-jakarta-stream"/>
```

3. Web アプリケーションサーバーを再起動します。

また他の方法として、デフォルトで定義されている※インターセプター「fileUpload」を使用せず、独自にカスタマイズしたインターセプタースタックを定義、使用することでも問題の回避は可能です。同対策は Apache Struts 2.5.8 から 2.5.10 までのバージョンでのみ有効です。
※Action が呼び出される前後に実行される処理。

インターセプターの設定手順は以下の通りです。なお、下記は弊社環境(Apache Struts 2.5.8 を使用)の場合での設定例です。詳細は以下開発元の Web サイトをご確認ください。
S2-046 – Apache Struts 2 Documentation – Apache Software Foundation

1. struts.xml に以下の内容を追記します。

```
<package name="default" extends="struts-default">
    <interceptors>
      <interceptor-stack name="defaultWithoutUpload">
       <interceptor-ref name="exception"/>
       <interceptor-ref name="alias"/>
       <interceptor-ref name="servletConfig"/>
       <interceptor-ref name="i18n"/>
       <interceptor-ref name="prepare"/>
       <interceptor-ref name="chain"/>
       <interceptor-ref name="scopedModelDriven"/>
       <interceptor-ref name="modelDriven"/>
       <interceptor-ref name="checkbox"/>
       <interceptor-ref name="datetime"/>
       <interceptor-ref name="multiselect"/>
       <interceptor-ref name="staticParams"/>
       <interceptor-ref name="actionMappingParams"/>
       <interceptor-ref name="params"/>
       <interceptor-ref name="conversionError"/>
       <interceptor-ref name="validation">
          <param name="excludeMethods">input,back,cancel,browse</param>
       </interceptor-ref>
       <interceptor-ref name="workflow">
          <param name="excludeMethods">input,back,cancel,browse</param>
       </interceptor-ref>
       <interceptor-ref name="debugging"/>
      </interceptor-stack>
    </interceptors>

   <default-interceptor-ref name="defaultWithoutUpload"/>
```

2. Web アプリケーションサーバーを再起動します。

【Apache Struts のバージョン確認方法】
Apache Struts 2 がインストールされた Web アプリケーションサーバーにて、/WEB-INF 以下にある.jar ファイルを検索します。検索結果として表示される struts2-core-2.x.x.jar の「2.x.x」の部分が、バージョン情報になります。
また、struts2-core-2.x.x.jar ファイルに含まれる MANIFEST.MF について、Bundle-Version から始まる行を参照することでも、Apache Struts 2 バージョン情報を確認することが可能です。

CentOS7 の場合での実行例

```
[root@localhost ~]# find /var/lib/tomcat/webapps/showcase/WEB-INF -name struts2-core*.jar
/var/lib/tomcat/webapps/showcase/WEB-INF/lib/struts2-core-2.3.31.jar
```

【参考サイト】

- S2-046 – Apache Struts 2 Documentation – Apache Software Foundation
- GitHub – apache/struts-extras

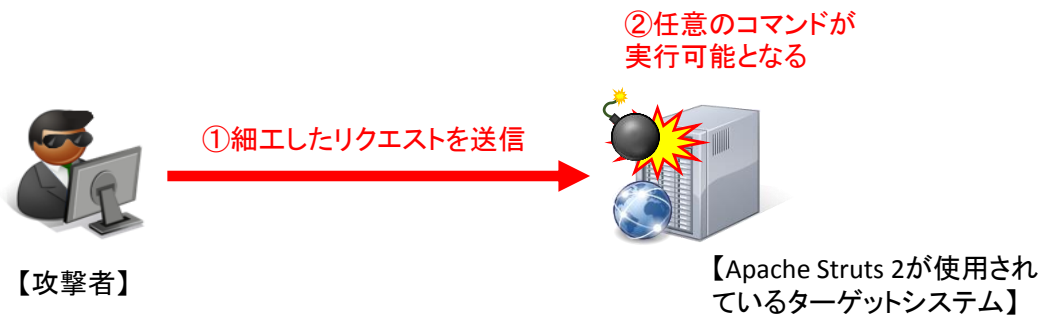
【検証概要】

攻撃者は、ターゲットシステムで動作する Web アプリケーションサーバーにインストールされた Apache Struts 2 へ細工を行ったリクエストを送信することにより、このターゲットシステムにて Web アプリケーションサーバーの実行権限で任意のコマンドが実行可能となります。

【検証ターゲットシステム】

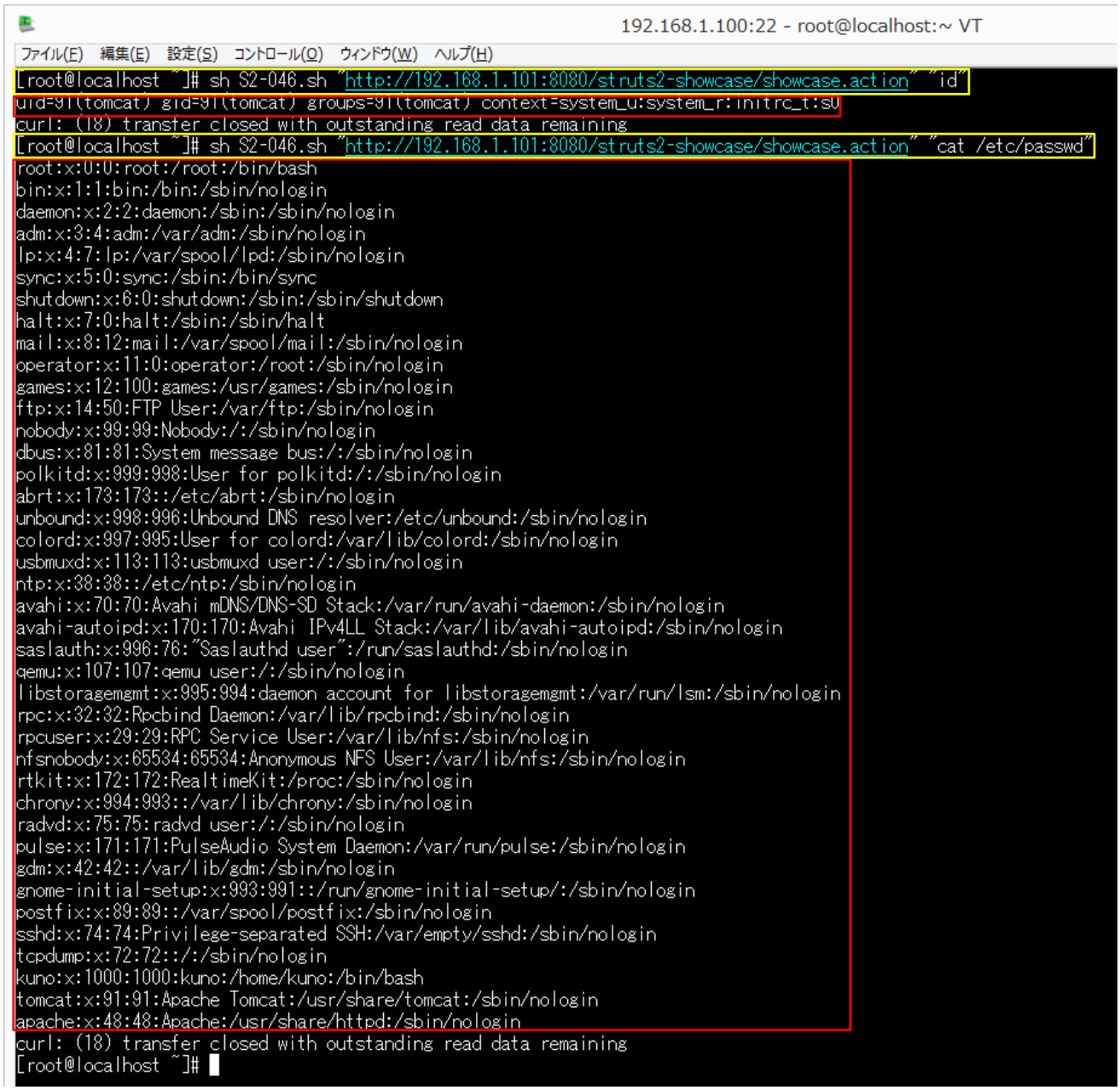
CentOS7.0 + Tomcat7.0.69 + Apache Struts 2.3.31

【検証イメージ】

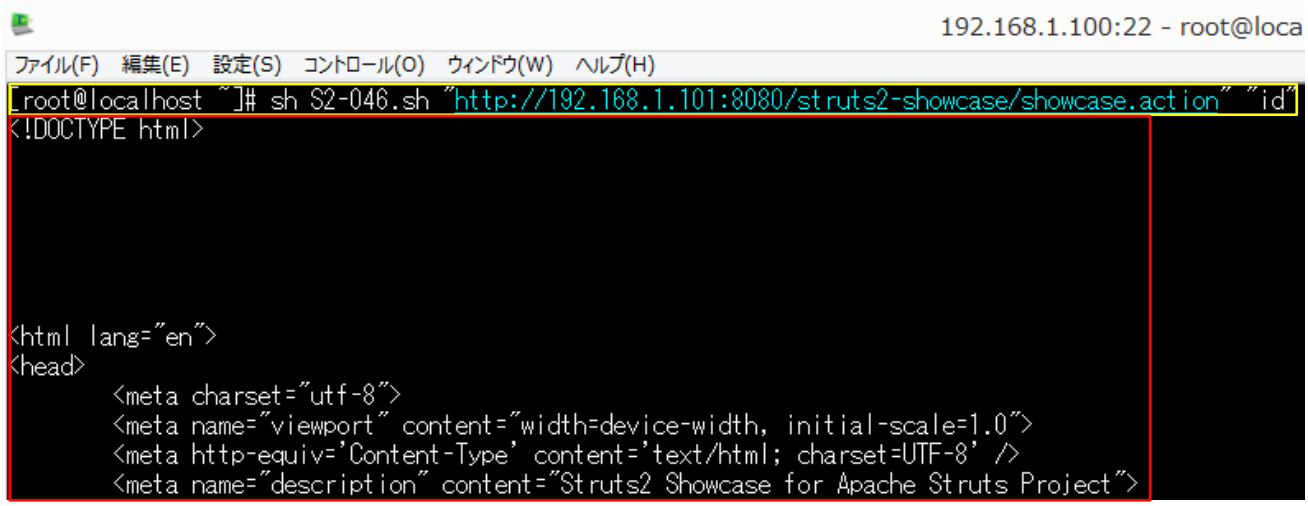


【検証結果】

下図は、ターゲットシステムに対して細工したリクエストを送信した際の画面です。黄枠の箇所は、ターゲットシステムに対して任意のコマンド（id は現在のユーザーの情報を表示するコマンド、cat /etc/passwd は/etc/passwd ファイルを参照するコマンド）を実行しています。一方で赤枠の箇所は、コマンドの実行結果（ユーザー情報の表示、および/etc/passwd ファイルの内容の表示）が表示されていることを確認できます。（以下の図では tomcat ユーザーによるコマンドの実行がされていますが、こちらの権限は Apache Struts 2 がインストールされた Web アプリケーションサーバーの実行権限に依存します）


192.168.1.100:22 - root@localhost:~ VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
[root@localhost ~]# sh S2-046.sh "http://192.168.1.101:8080/struts2-showcase/showcase.action" "id"
uid=91(tomcat) gid=91(tomcat) groups=91(tomcat) context=system_u:system_r:initrc_t:s0
curl: (18) transfer closed with outstanding read data remaining
[root@localhost ~]# sh S2-046.sh "http://192.168.1.101:8080/struts2-showcase/showcase.action" "cat /etc/passwd"
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
unbound:x:998:996:Unbound DNS resolver:/etc/unbound:/sbin/nologin
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
saslauth:x:996:76:"Saslauthd user":/run/saslauthd:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
libstoragemgmt:x:995:994:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
chrony:x:994:993::/var/lib/chrony:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:993:991::/run/gnome-initial-setup/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
kuno:x:1000:1000:kuno:/home/kuno:/bin/bash
tomcat:x:91:91:Apache Tomcat:/usr/share/tomcat:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
curl: (18) transfer closed with outstanding read data remaining
[root@localhost ~]#

なお、上記対策案のプラグインを設定した場合には、以下の通り任意のコマンドが実行できず攻撃が成立しないことが確認できました。



【更新履歴】

2017 年 3 月 28 日 ： 初版公開

ソフトバンク・テクノロジー株式会社
〒160-0022 東京都新宿区新宿 6 丁目 27 番地 30 号
新宿イーストサイドスクエア 17 階
受付時間：平日 10:00～17:00
電話 03-6892-3154
メール sbt-ipsol@tech.softbank.co.jp
URL https://www.softbanktech.jp/