

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-2016-3081)(S2-032)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-2016-3081)(S2-032)及び、その脆弱性を利用する攻撃ツールが発見されました。この脆弱性は、Dynamic Method Invocation に起因する脆弱性であり、同機能が有効である場合にのみ影響を受けます。

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 Struts 2 が配置された 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(2016年4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(2016年4月19日付)。しかしながら、攻撃が容易であること、また攻撃を受けた際にシステムへの影響が大きいことから、今回、この脆弱性(CVE-2016-3081)の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 2.3.20.3 および 2.3.24.3 を除く、2.3.20 から 2.3.28 までのバージョン

【対策案】

本レポート作成(2016年4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。アップグレードが困難である場合、Dynamic Method Invocation 機能を無効化することにより問題を回避することが可能です。Dynamic Method Invocation 機能を無効化するためには、struts.xml 内の『struts.enable.DynamicMethodInvocation』の設定値を『false』にした後、Web アプリケーションサーバーを再起動します。

(設定例)

```
<constant name="struts.enable.DynamicMethodInvocation" value="false" />
```

【バージョン確認方法】

Apache Struts 2 が配置された Web アプリケーションサーバーにて、/WEB-INF/lib 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.x.jar の『2.x.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.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。

【参考サイト】

- [CVE-2016-3081](#)
- [Apache Struts2 の脆弱性対策について\(CVE-2016-3081\)\(S2-032\)](#)

【検証概要】

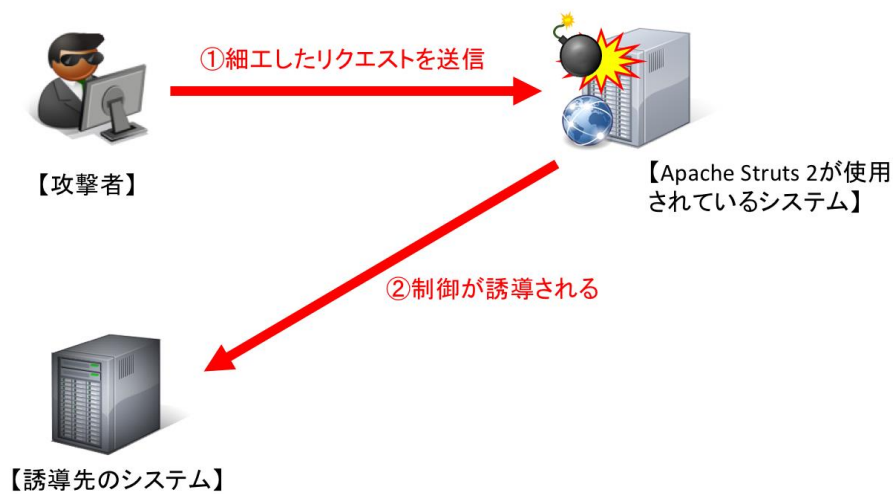
攻撃者は、ターゲットシステムで動作する Web アプリケーションサーバーに配置された Apache Struts 2 へ細工を行ったパケットを送信することにより、このターゲットから誘導先のシステムへコネクションを確立させます。この結果、誘導先のシステムより Web アプリケーションサーバーの実行権限で任意のコマンドが実行可能となります。

*誘導先のシステムは Windows 7 Professional です。

【検証ターゲットシステム】

Debian 7 上で動作する Tomcat 7.0.39 に配置された Apache Struts 2.3.24

【検証イメージ】



【検証結果】

下図は、誘導先のシステム (Windows 7) 上で攻撃用のツールを実行した際の画面です。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 (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 が配置された Web アプリケーションサーバーの実行権限に依存します)

```

命令: cat /etc/passwd
-----
★K8cmd-> id
uid=109(tomcat) gid=115(tomcat) groups=115(tomcat)

★K8cmd-> cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailin List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization.../run/systemd/bin/false
systemd-networkd:x:101:104:systemd Network Management.../run/systemd/netif/bin/false
systemd-resolved:x:102:105:systemd Resolver.../run/systemd/resolve/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy.../run/systemd/bin/false
Debian-exim:x:104:109:/var/spool/exim4:/bin/false
messagebus:x:105:110:/var/run/dbus:/bin/false
statd:x:106:65534:/var/lib/ntfs:/bin/false
sshd:x:107:65534:/var/run/ssh:/usr/sbin/nologin
testuser:x:1000:1000:testuser.../home/testuser:/bin/bash
bind:x:53:53:/var/named:/sbin/nologin
mysql:x:108:113:MySQL Server.../nonexistent/bin/false
tomcat:x:109:115:/opt/tomcat/bin/false

```

【更新履歴】

2016 年 4 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/