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」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

【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)(S2-045)及び、その脆弱性を利用する攻撃コードおよびツールが発見されました。この脆弱性は、ファイルアップロード時に使用するマルチパーサー「jakarta」に起因する脆弱性で、同マルチパーサーは Apache Struts 2 にてデフォルトで使用しているものです。
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(2017 年 3 月 8 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、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-2017-5638)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 2.3.5 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 8 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。

(2017 年 3 月 28 日追記)

本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、「S2-046」の影響を受けます。そのため、ただちにアップグレードすることが困難である場合には、以下レポートの対策案を実施いただくことで、「S2-045」および「S2-046」の問題を回避することが可能です。
「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」

【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 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】

- CVE-2017-5638
- S2-045 - Apache Struts 2 Documentation - Apache Software Foundation

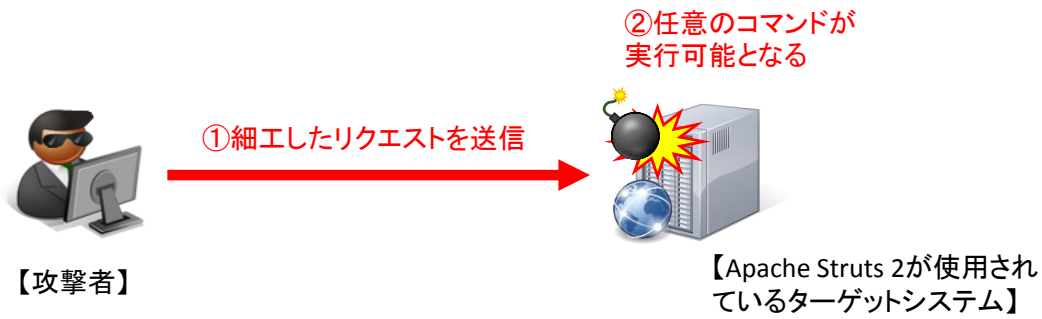
【検証概要】

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

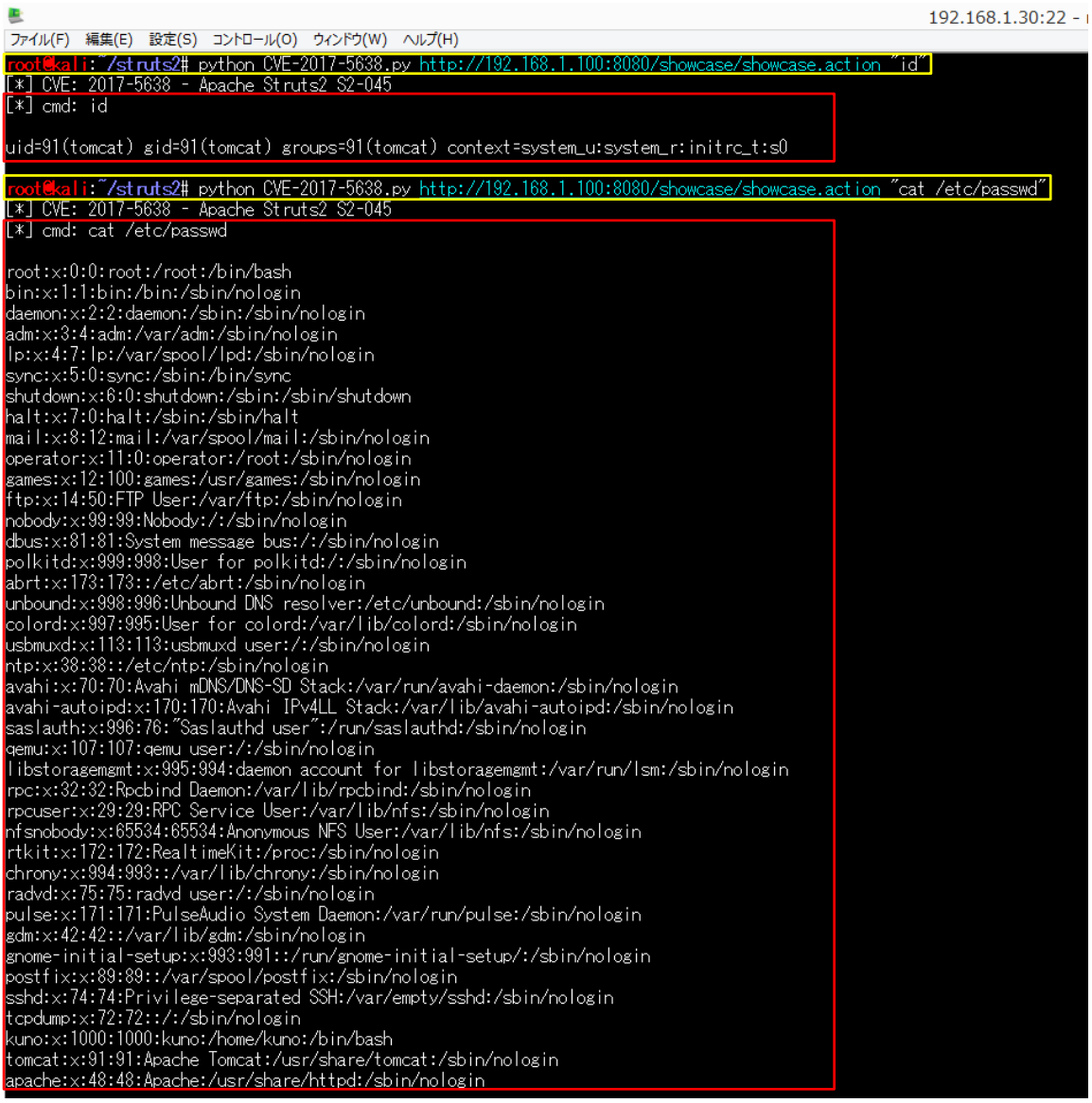
【検証イメージ】



【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）



【更新履歴】

2017 年 3 月 8 日 ： 初版公開

2017 年 3 月 28 日 ： 対策案に「S2-046」に関する内容を追記

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/