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 Struts REST プラグインの脆弱性により、リモートから任意のコードが実行可能な脆弱性(CVE-2017-9805)(S2-052)に関する調査レポート

【概要】

Apache Struts 2 の Struts REST プラグインに、リモートより任意のコードが実行可能な脆弱性(CVE-2017-9805)(S2-052)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。

本脆弱性は、Struts REST プラグインが XML リクエストを処理する際の不具合に起因する脆弱性で、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 9 月 8 日)時点において、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(Apache Struts 2.5.3 は 2017 年 9 月 5 日付、Apache Struts 2.3.34 は 2017 年 9 月 7 日付(ともに米国時間))。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-2017-9805)(S2-052)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 2.1.2 から 2.3.33 までのバージョン
- Apache Struts 2.5 から 2.5.12 までのバージョン

【対策案】

本レポート作成(2017 年 9 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。

【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 /lib/tomcat/webapps/struts2-rest-showcase/WEB-INF -name struts2-core*.jar
/lib/tomcat/webapps/struts2-rest-showcase/WEB-INF/lib/struts2-core-2.3.33.jar
```

【参考サイト】

- S2-052
- Announcements - Apache Struts - The Apache Software Foundation!
- CVE-2017-9805
- Apache Struts2 の脆弱性対策について(CVE-2017-9805)(S2-052)

【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、ターゲットシステムの脆弱性を利用して任意のコードを実行させます。

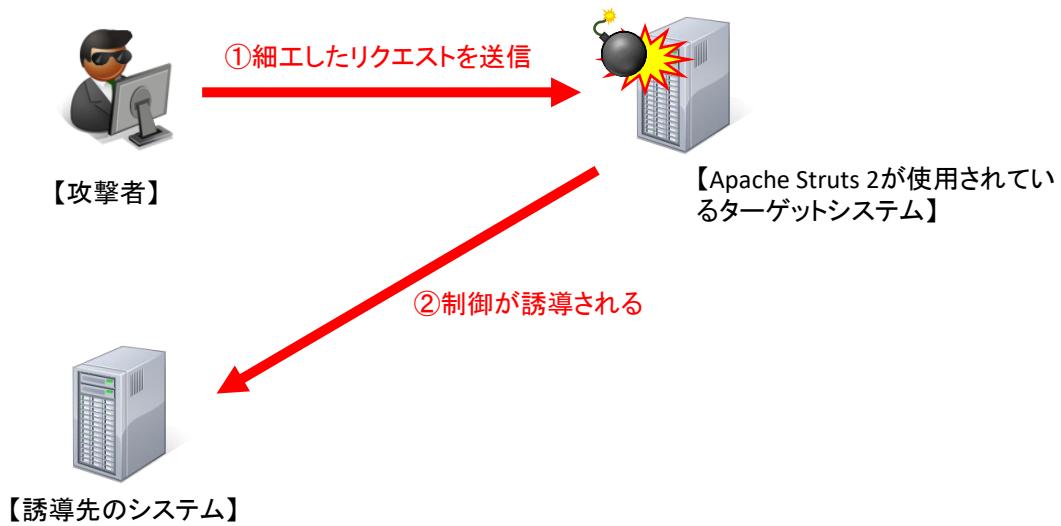
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートへコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートから Web アプリケーションサーバーの実行権限でターゲットシステムが操作可能となります。

*誘導先のシステムは Debian です。

【検証ターゲットシステム】

- CentOS7.0 + Tomcat 8.5.20 + Apache Struts 2.3.33
- CentOS7.0 + Tomcat 8.5.20 + Apache Struts 2.5.12

【検証イメージ】

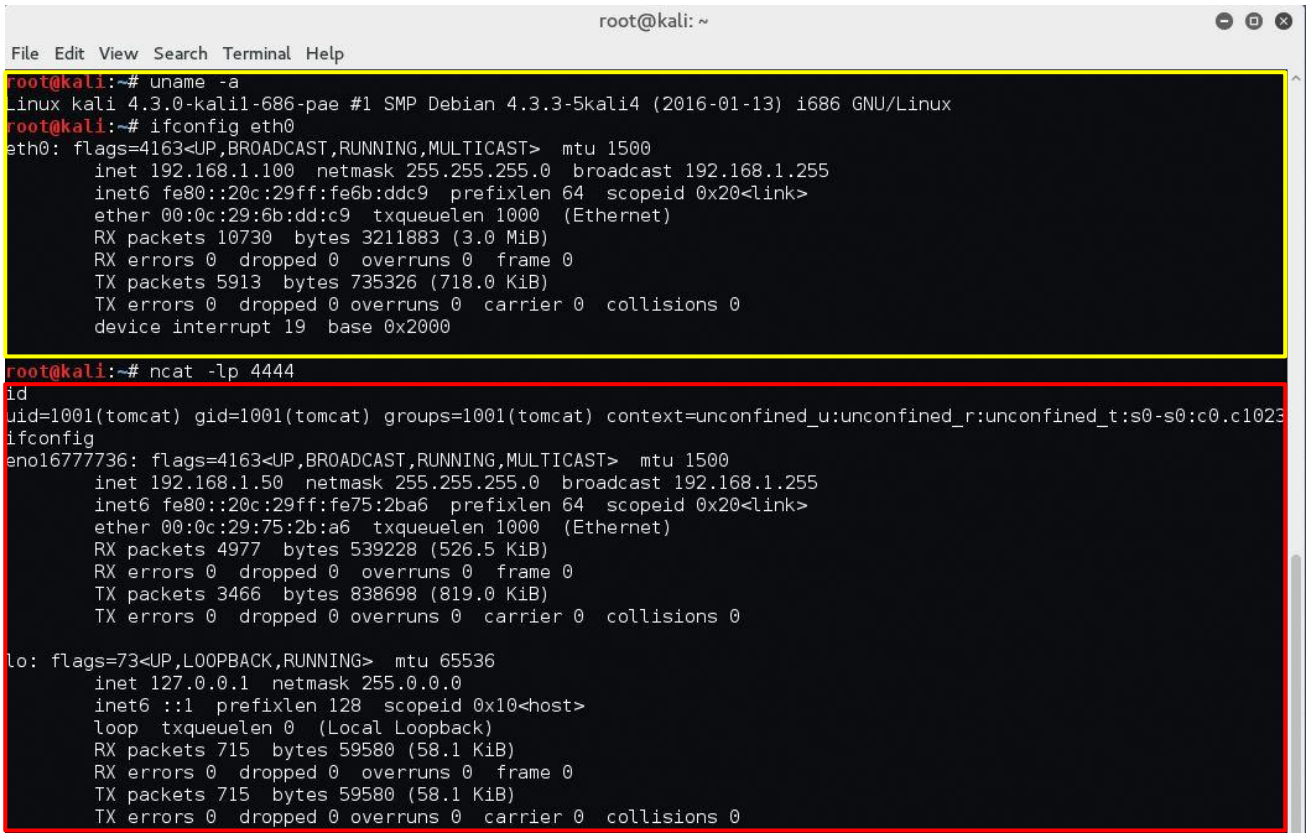


【検証結果】

下図は、誘導先のコンピュータ(Debian)の画面です。黄線で囲まれた部分は、誘導先のホストの情報です。

一方で、赤線で囲まれている部分は、ターゲットシステム(CentOS)において、ユーザーの情報、IP アドレスの情報を表示する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で任意のコマンドを実行することに成功したと判断できます。



【更新履歴】 2017 年 9 月 8 日 ： 初版公開

【本レポートに関するお問い合わせ先】

■報道関係者様からのお問い合わせ

経営企画部 コーポレートコミュニケーショングループ

TEL：03-6892-3063 ／ Email： sbt-pr@tech.softbank.co.jp

■お客様からのお問い合わせ

下記フォームよりお問い合わせください。

https://info.softbanktech.jp/public/application/add/508