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 の脆弱性により、リモートから任意のコードを実行可能な脆弱性(CVE-2018-11776)(S2-057)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-2018-11776)(S2-057)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、Struts フレームワークのコアによるデータ検証処理の欠陥にあり、alwaysSelectFullNamespace が true に設定されている場合、または、struts の設定ファイルにワイルドカード namespace を使用した action タグまたは url タグが含まれる場合に影響を受けます。
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(2018 年 8 月 27 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(2018 年 8 月 22 日付)。しかしながら、攻撃が容易であり、かつ攻撃コードも公開されていること、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-2018-11776)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 から 2.3.34 までのバージョン
- Apache Struts 2.5 から 2.5.16 までのバージョン

上記以外のサポート外のバージョンの Struts でも、脆弱性の影響を受ける可能性があります。

【対策案】

本レポート作成(2018 年 8 月 27 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/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-2018-11776

- Apache Struts2 の脆弱性対策について(CVE-2018-11776)(S2-057)
- S2-057 - Apache Struts 2 Documentation - Apache Software Foundation

【検証概要】

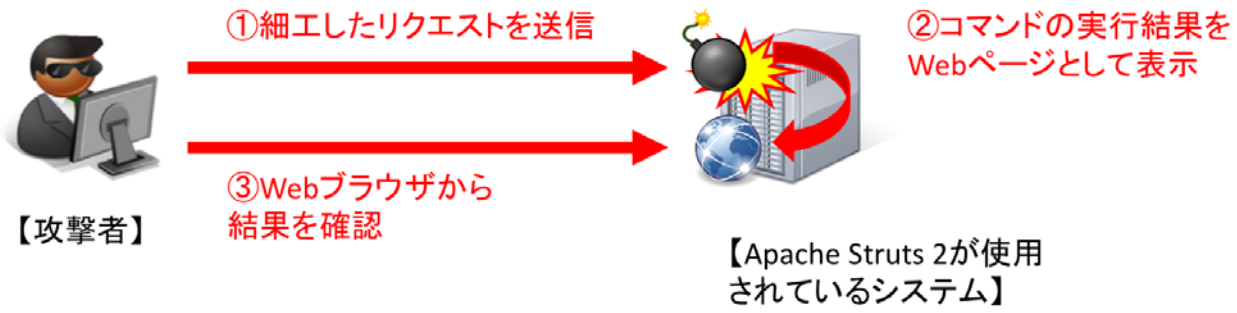
攻撃者は、ターゲットシステムで動作する Web アプリケーションサーバーに配置された Apache Struts 2 へ細工を行ったパケットを送信することにより、Web アプリケーションサーバーの実行権限で任意のコードを実行させます。その後、Web ブラウザでアクセスすることにより、任意のコードの実行結果を確認します。

【検証ターゲットシステム】

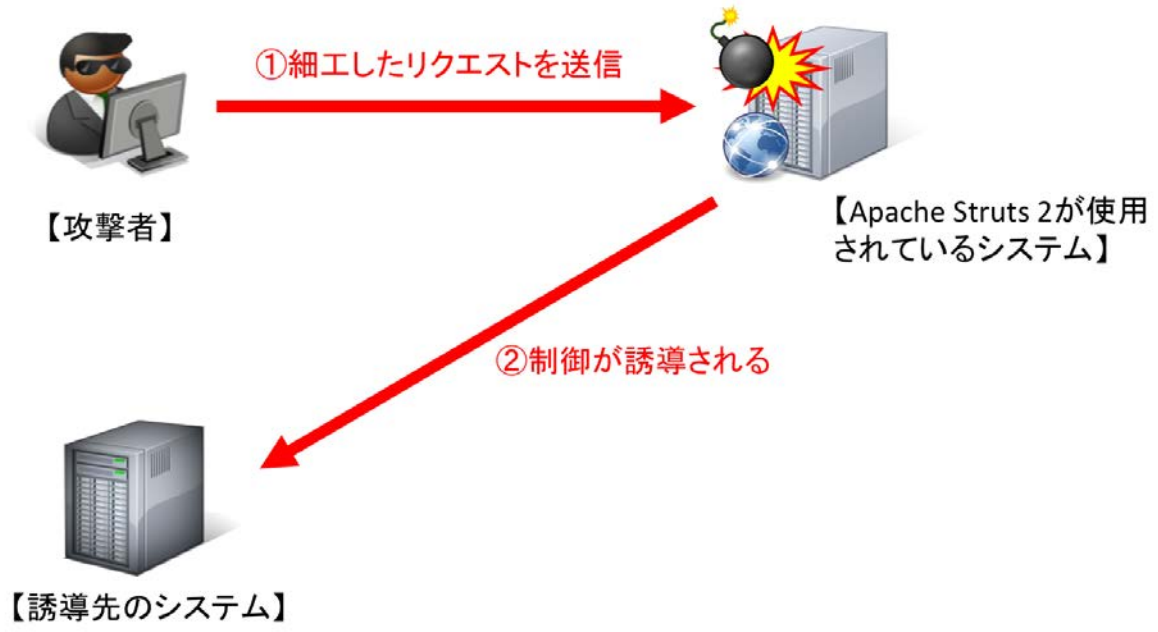
Debian 9 上で動作する Tomcat 8.5.33 に配置された Apache Struts 2.3.14

【検証イメージ】

・検証 1



・検証 2

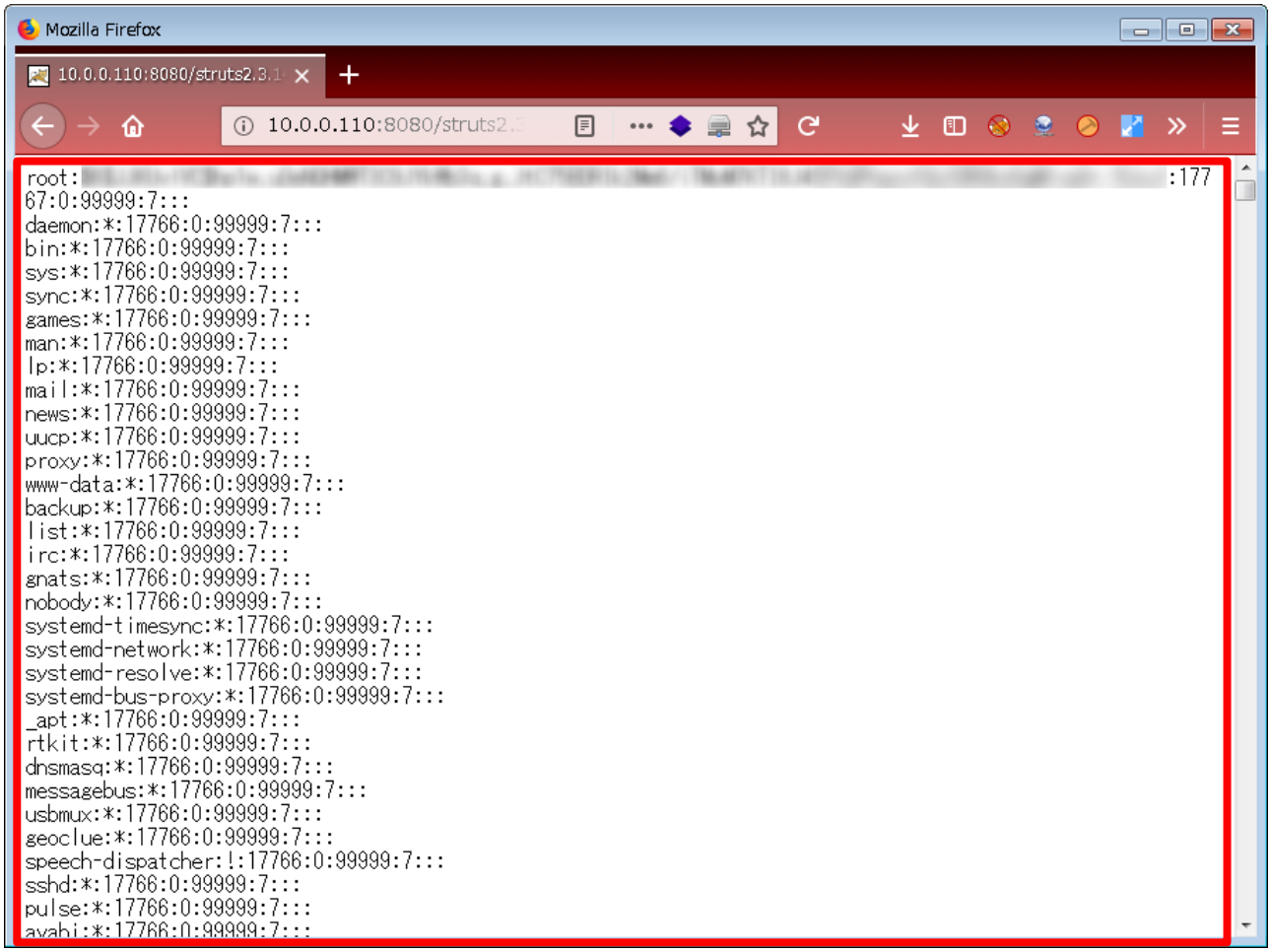


【検証結果】

・検証 1

下図は、ターゲットシステム（Debian）にて root 権限で動作する Web アプリケーションサーバーに対して、ブラウザでアクセスした際の画面です。赤線で囲まれている部分は、ターゲットシステムの/etc/shadow の内容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。

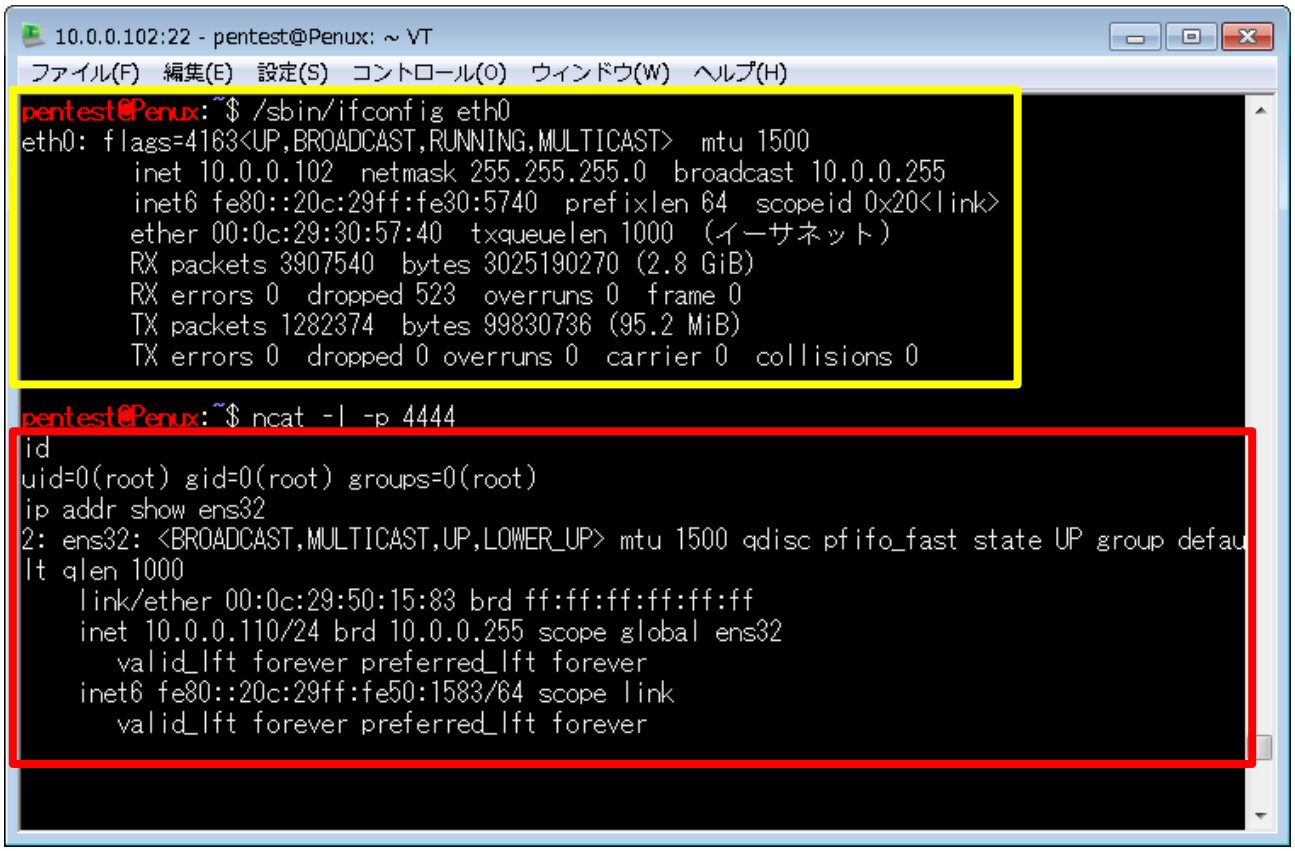


・検証 2

また、ターゲットシステムの制御を誘導先システムから奪取する検証も行いました。

以下の画面の黄線で囲まれた部分は、誘導先のシステムの情報、一方で、赤線で囲まれている部分は、ターゲットシステムにおけるユーザー情報、ホストのネットワーク情報を表示するコマンドを実行した結果です。

この結果、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】

2018 年 8 月 27 日 ： 初版公開

『報道関係者様からのお問い合わせ』

ソフトバンク・テクノロジー株式会社

管理本部　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

メールアドレス：sbt-pr@tech.softbank.co.jp