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が実行可能な脆弱性（CVE-2016-4438）（S2-037）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-2016-4438）（S2-037）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、REST Plugin に起因する脆弱性であり、同 Plugin を利用しているコンテンツ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 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（2016 年 6 月 22 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 6 月 17 日付）。しかしながら、攻撃が容易であり、攻撃ツール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-2016-4438）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 から 2.3.28.1 までのバージョン

【対策案】

本レポート作成（2016 年 6 月 22 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-2016-4438
- Apache Struts 2 の脆弱性（S2-037）に関する注意喚起

【検証概要】

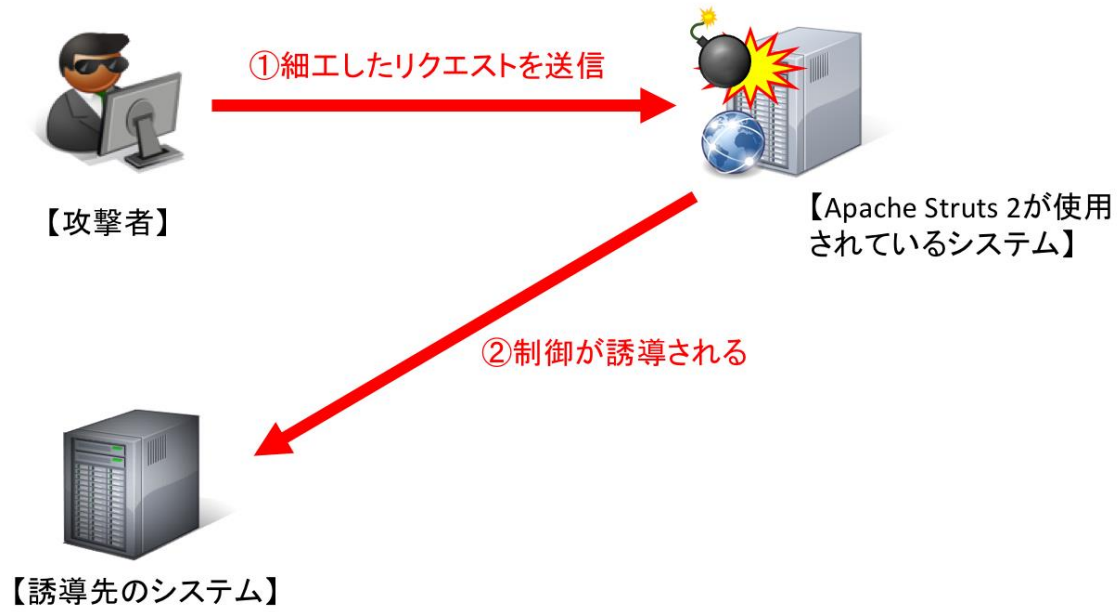
攻撃者は、ターゲットシステムで動作する Web アプリケーションサーバーに配置された Apache Struts 2 へ細工を行ったパケットを送信することにより、このターゲットから誘導先のシステムへコネクションを確立させます。この結果、誘導先のシステムより Web アプリケーションサーバーの実行権限で任意のコマンドが実行可能となります。

*誘導先のシステムは Windows 8.1 Pro です。

【検証ターゲットシステム】

Debian 8 上で動作する Tomcat 7.0.39 に配置された Apache Struts 2.3.28

【検証イメージ】

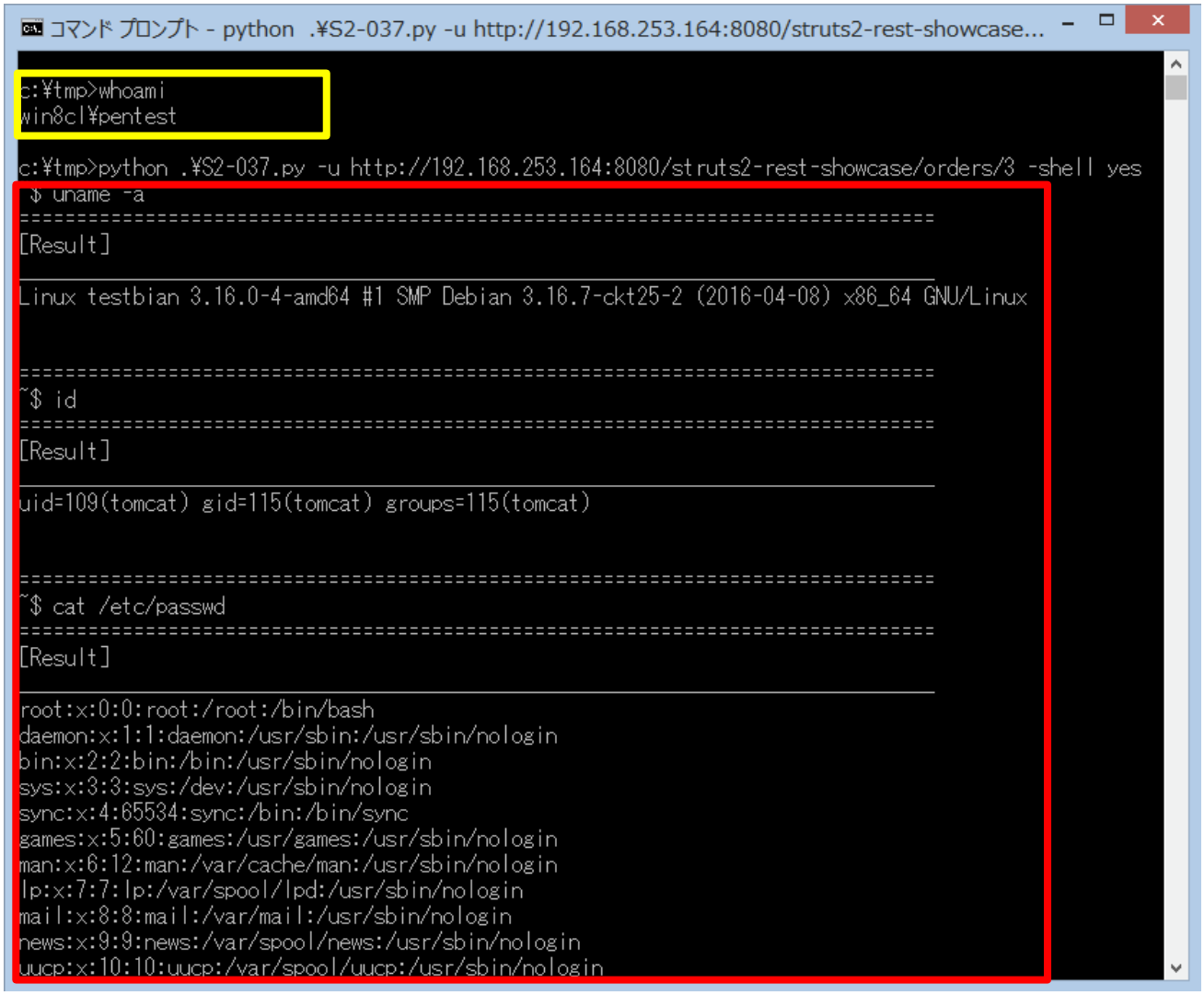


【検証結果】

下図は、誘導先のシステム（Windows 8.1）上の画面です。黄線で囲まれた部分は、誘導先のホスト名、および、攻撃コードを実行するユーザー名が表示されています。

一方で、赤線で囲まれている部分は、ターゲットシステムにおいて、カーネル情報、ユーザー情報、/etc/passwd ファイル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。（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 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に依存します）

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】

2016 年 6 月 22 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/