NTT DATA
NTTデータ 先端技術株式会社

Apache Struts 2 の includeParams による入力値処理の不備により 任意の Java コードが実行される脆弱性 (CVE-2013-1966)に関する検証レポート

2013/5/28
NTT データ先端技術株式会社
辻　伸弘
小松　徹也

【概要】

Apache Struts 2 に、任意の Java コードが実行される脆弱性が存在します。
この脆弱性は、includeParams による入力値処理時において、値を OGNL 式（※）として評価するため、任意の Java コードを実行可能です。

この脆弱性を悪用して、攻撃者はターゲットホスト上にて、Web サーバの動作権限で任意の Java コードの実行が可能です。
今回、この Apache Struts 2 の includeParams による入力値処理の不備により任意の Java コードが実行される脆弱性（CVE-2013-1966）の再現性について検証を行いました。

※Object Graph Navigation Language
Java オブジェクトのプロパティへアクセス時に利用する式言語

【影響を受けるとされているシステム】

影響を受ける可能性が報告されているのは次の通りです。
- Apache Struts 2.0.0 から 2.3.14.1

【対策案】

当該脆弱性が修正された最新版 Apache Struts 2 にアップデートしていただく事を推奨いたします。

本脆弱性は、Apache Struts 2.3.14.1 にて修正されたとの情報がありました。しかしながら、攻撃手法の変更により、攻撃が可能であり修正が不十分であることが報告されています。
そのため、再度公開された Apache Struts 2.3.14.2 を利用する必要があることに注意してください。

公開されたバージョン	脆弱性（CVE-2013-1966）の修正状況
Apache Struts 2.3.14 以前	未修正
Apache Struts 2.3.14.1	未修正
Apache Struts 2.3.14.2	修正

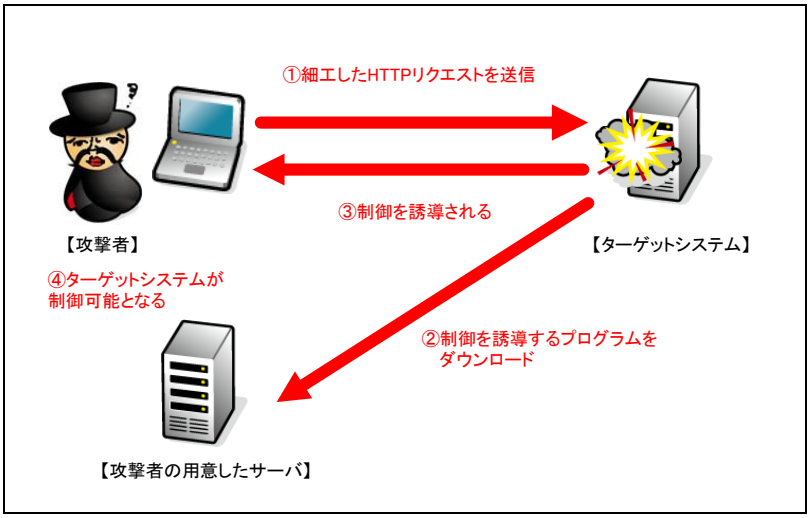
Apache Struts Releases
http://struts.apache.org/downloads.html

【参考サイト】

CVE-2013-1966
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1966

Apache Struts "ParameterInterceptor" Security Bypass Vulnerability
http://secunia.com/advisories/53495/

【検証イメージ】



【検証ターゲットシステム】

Debian 6.0.7 上の Tomcat 7.0.40、Apache Struts 2.3.14 および Apache Struts 2.3.14.1 を利用した Web アプリケーション

【検証概要】

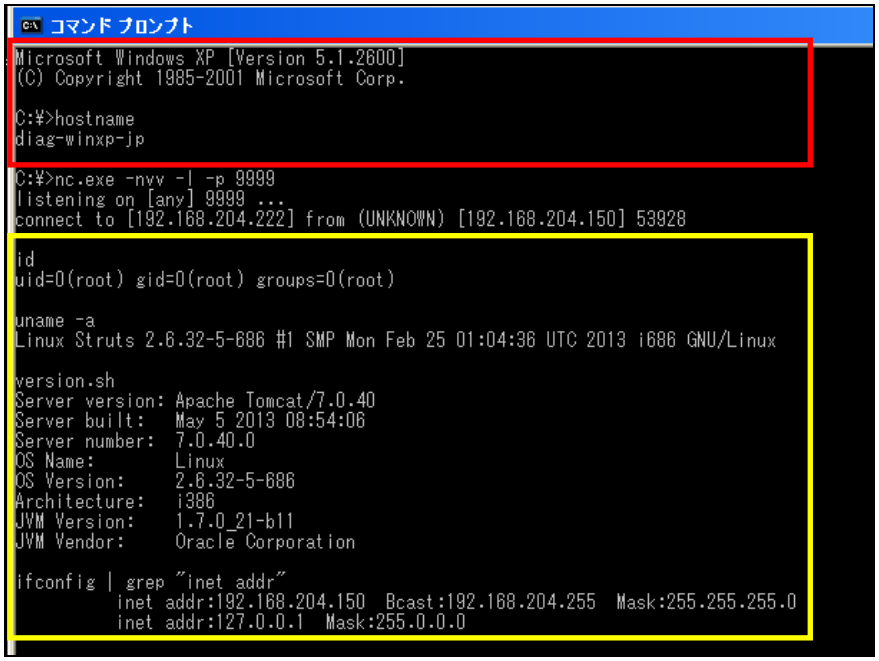
ターゲットシステムに、細工した HTTP リクエストを送信し、Struts を利用したアプリケーションを介して、Web サーバの動作権限で任意の Java コードを実行させます。
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバより、プログラムのダウンロードを行なった上で、そのプログラムを用いて、特定サーバのポートへコネクションを確立させるように誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムを操作可能となります。
＊誘導先のシステムは Windows XP です。

【検証結果】

下図の赤線で囲まれている部分の示すように、誘導先のコンピュータ（Windows XP）のコンソール上にターゲットシステム（Debian）のプロンプトが表示されています。
黄線で囲まれている部分の示すように、ターゲットシステムにおいて、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の制御の奪取に成功したと言えます。

NTTデータ 先端技術株式会社

ターゲットシステムの制御の奪取に成功した画面



＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ先端技術株式会社
セキュリティ事業部
TEL：03-5859-5422
http://security.intellilink.co.jp