NTT DATA
NTTデータ 先端技術株式会社

Apache Struts の Exception Delegator におけ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-2012-0391）に関する検証レポート

2012/6/22
NTT データ先端技術株式会社
辻　伸弘
小松　徹也

【概要】

Apache Struts 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、Exception Delegator における入力値処理時の例外において、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、奪取されたユーザ権限で任意の Java コードの実行が可能です。
今回、この Apache Struts の Exception Delegator におけ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-2012-0391）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 2.2.3 およびそれ以前のバージョン

【対策案】

当該脆弱性が修正された最新版 Apache Struts 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、2.2.3.1 以降にて対策済みです。

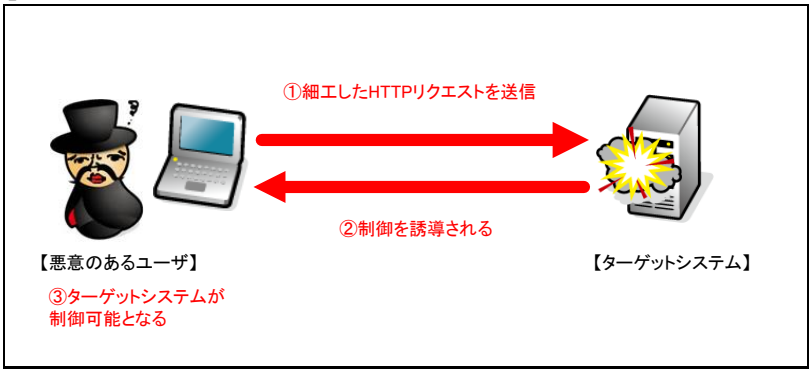
Apache Struts Releases
http://struts.apache.org/downloads.html

【参考サイト】

CVE-2012-0391
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0391

Apache Struts: Security Bulletins > S2-008
http://struts.apache.org/2.x/docs/s2-008.html

【検証イメージ】

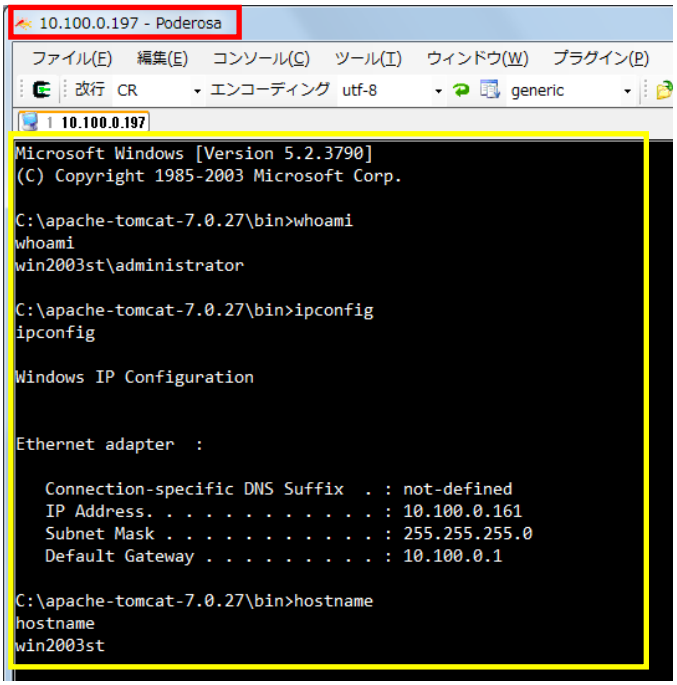


【検証ターゲットシステム】
Windows Server 2003 上の Tomcat 7.0.27、Apache Struts 2.2.1.1 を利用した Web アプリケーション
Debian 6.0.2 上の Jetty 6.1.25、Apache Struts2.2.1.1 を利用した Web アプリケーション

【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、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、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 Debian 5.05 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（Debian）のコンソール上にターゲットシステム（Windows Server 2003）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。

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　営業担当　サービス企画戦略グループ
TEL:03-5859-5422
http://security.intellilink.co.jp