

Apache Struts2 の prefix パラメータ処理の不備により 任意の Java コードが実行される脆弱性 (CVE-2013-2251) に関する検証レポート

2013/7/23

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、DefaultActionMapper における prefix パラメータ処理時において、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、AP 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 prefix パラメータ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-2013-2251) 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 2.3.15

【対策案】

この脆弱性が修正された最新版 Apache Struts2 にアップデートしていただく事を推奨いたします。この脆弱性は、2.3.15.1 以降にて対策済みです。

Apache Struts Releases

<http://struts.apache.org/downloads.html>

弊社の検査において、一般ユーザ権限でサーバを動作させていないシステムも見受けられます。この脆弱性は、AP サーバの動作権限を奪取されることから、管理者権限ユーザで AP サーバを動作させている場合、システムへの影響範囲が広がります。そのため、運用上必要かつ適切な権限にて動作させることを推奨します。

【参考サイト】

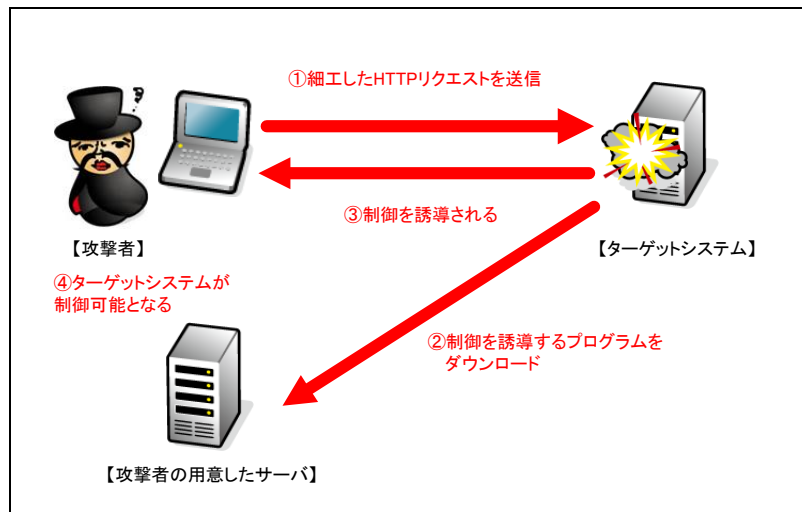
CVE-2013-2251

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2251>

Apache Struts DefaultActionMapper Redirection and OGNL Security Bypass Vulnerabilities

<http://secunia.com/advisories/54118>

【検証イメージ】



【検証ターゲットシステム】

- ・ Debian 6.0.7 上の Apache Tomcat 7.0.42、Apache Struts 2.3.15 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、AP 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が操作可能となります。

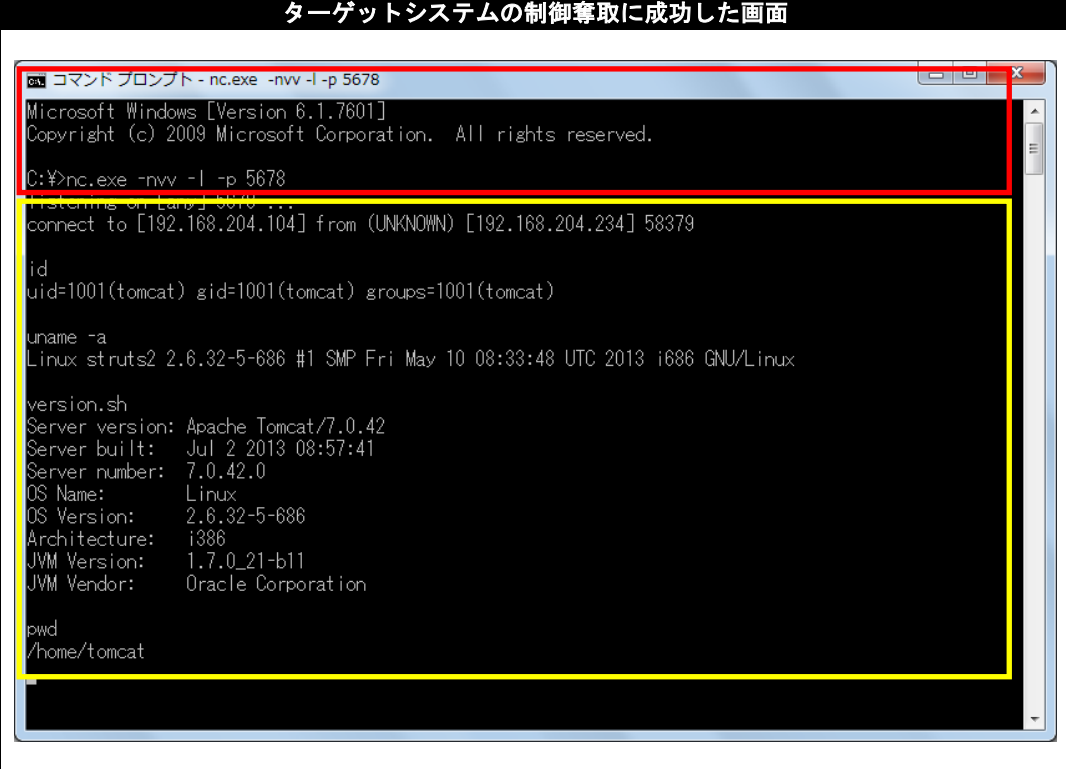
* 誘導先のシステムは Windows 7 です。

【検証結果】

下図は、攻撃後の誘導先のシステム画面です。

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 7）のターミナル上にターゲットシステム（Debian 6.0.7）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奪取に成功した画面



```
コマンドプロンプト - nc.exe -nvv -l -p 5678
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>nc.exe -nvv -l -p 5678
listening on [tcp://0.0.0.0:5678] ...
connect to [192.168.204.104] from (UNKNOWN) [192.168.204.234] 58379

id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)

uname -a
Linux struts2 2.6.32-5-686 #1 SMP Fri May 10 08:33:48 UTC 2013 i686 GNU/Linux

version.sh
Server version: Apache Tomcat/7.0.42
Server built: Jul 2 2013 08:57:41
Server number: 7.0.42.0
OS Name: Linux
OS Version: 2.6.32-5-686
Architecture: i386
JVM Version: 1.7.0_21-b11
JVM Vendor: Oracle Corporation

pwd
/home/tomcat
```

* 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>