



## Oracle Java SE、Java for Business のアプレット Applet2ClassLoader の脆弱性 (CVE-2010-4452)に関する検証レポート

2011/3/29  
NTT データ・セキュリティ株式会社  
辻 伸弘  
小田切 秀暁

### 【概要】

Oracle Java SE、Java for Business のアプレット Applet2ClassLoader に脆弱性 (CVE-2010-4452) が存在することが発見されました。  
この脆弱性により、細工された Web ページの閲覧などで、ローカルユーザと同じ権限が奪取される危険性があります。  
想定される被害としては、ローカルユーザ権限での情報取得、改ざん、または、ワームやスパイウェアなどの悪意あるプログラムをシステム内にインストールされることが考えられます。

今回、Oracle Java SE、Java for Business の脆弱性 (CVE-2010-4452) の再現性について検証を行いました。

### 【影響を受けるとされているシステム】

- ・ Java SE の下記バージョン
  - Windows、Solaris 及び Linux で動作する JDK/JRE 6 Update 23 以前
  - Solaris 9 で動作する JDK 5.0 Update 27 以前
  - Solaris 8 で動作する SDK 1.4.2\_29 以前
- ・ Java Business の下記のバージョン
  - Windows、Solaris 及び Linux で動作する JDK/JRE 6 Update 23 以前
  - Windows、Solaris 及び Linux で動作する JDK/JRE 5.0 Update 27 以前
  - Windows、Solaris 及び Linux で動作する SDK/JRE 1.4.2\_29 以前

### 【対策案】

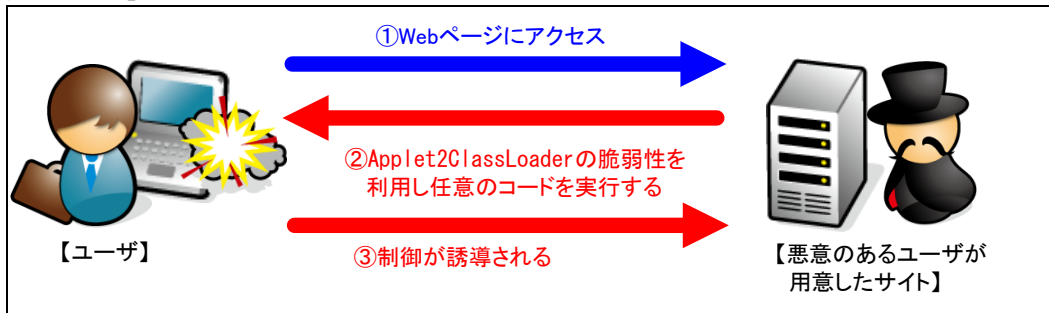
Java SE、Java Business のアップデートを実施いただく事を推奨いたします。

- ・ Java SE
  - Windows、Solaris 及び Linux で動作する JDK/JRE 6 Update 24
  - Solaris 9 で動作する JDK 5.0 Update 28
  - Solaris 8 で動作する SDK 1.4.2\_30
- ・ Java Business
  - Windows、Solaris 及び Linux で動作する JDK/JRE 6 Update 24
  - Windows、Solaris 及び Linux で動作する JDK/JRE 5.0 Update 28
  - Windows、Solaris 及び Linux で動作する SDK/JRE 1.4.2\_30

### 【参考サイト】

Oracle Java SE and Java for Business Critical Patch Update Advisory – February 2011  
<http://www.oracle.com/technetwork/topics/security/javacpufeb2011-304611.html>  
CVE-2010-4452  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-4452>

【検証イメージ】



【検証ターゲットシステム】

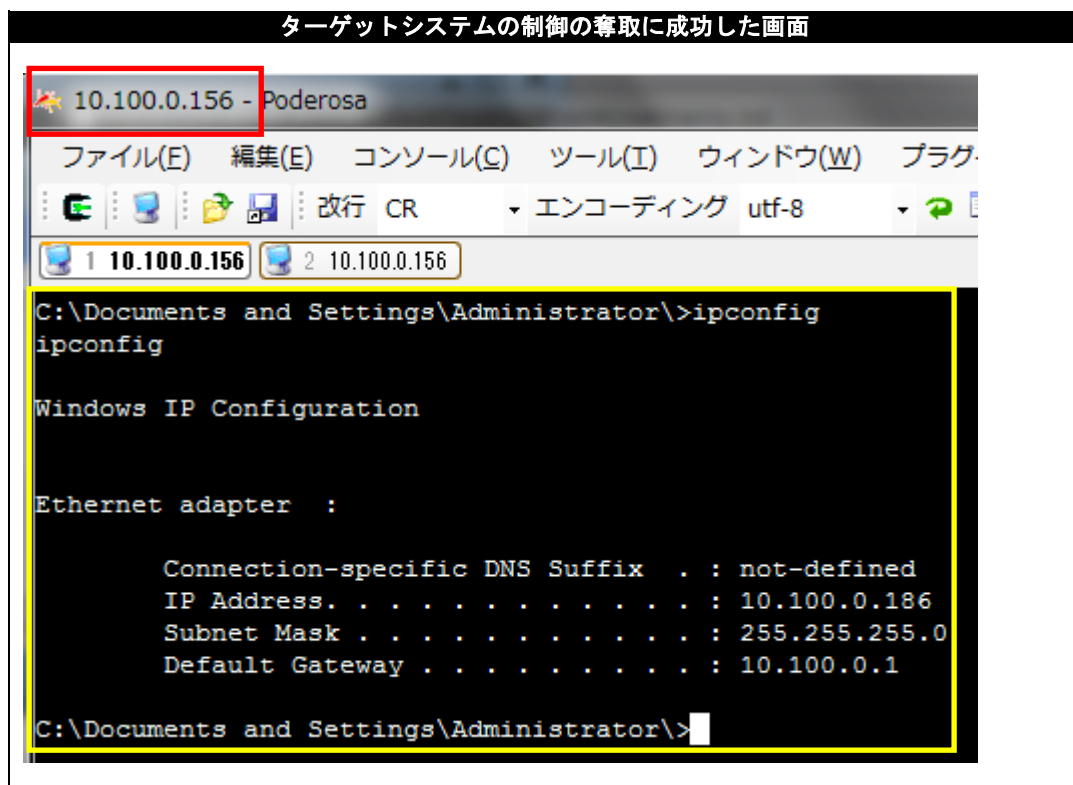
Windows XP SP3 IE7 JRE 6 Update 23

【検証概要】

ターゲットシステムに、細工した Web コンテンツをロードさせることで任意の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 XP) 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・セキュリティ株式会社

\* 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・セキュリティ株式会社

企画部 広報グループ

TEL:03-5425-1954

<http://www.nttdata-sec.co.jp/>