NTTデータ先端技術株式会社

Oracle Java SE JDK および JRE の Deployment サブコンポーネントにおける 脆弱性（CVE-2012-0500)に関する検証レポート

2012/2/28
NTT データ先端技術株式会社
辻 伸弘
小田切 秀暁

【概要】

Oracle Java SE JDK および JRE の Deployment サブコンポーネントに、任意のコードが実行される脆弱性（CVE-2012-0500）が存在します。この脆弱性は、JNLP ファイル内で実行パラメータを処理する際に発生する入力検証エラーに起因します。これにより、悪質な JNLP ファイルを処理させることで、攻撃可能な状態となります。

この脆弱性を悪用して、攻撃者はターゲットホスト上で任意のコードの実行が可能です。攻撃者は、巧妙に細工された Java Applet または Java Web Start アプリケーションを提供する Web サイトにユーザを誘導することで、この脆弱性を悪用します。

想定される被害としては、奪取されたユーザ権限による情報取得、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 JDK および JRE の脆弱性（CVE-2012-0500）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アプリケーション】

- Oracle Java JDK and JRE 7 Update 2 およびそれ以前
- Oracle Java JDK and JRE 6 Update 30 およびそれ以前
- Oracle JavaFX 2.0.2 およびそれ以前

【対策案】

Oracle 社より、この脆弱性を修正したバージョンがリリースされております。
当該脆弱性が修正されたバージョンにアップデートしていただくことを推奨いたします。

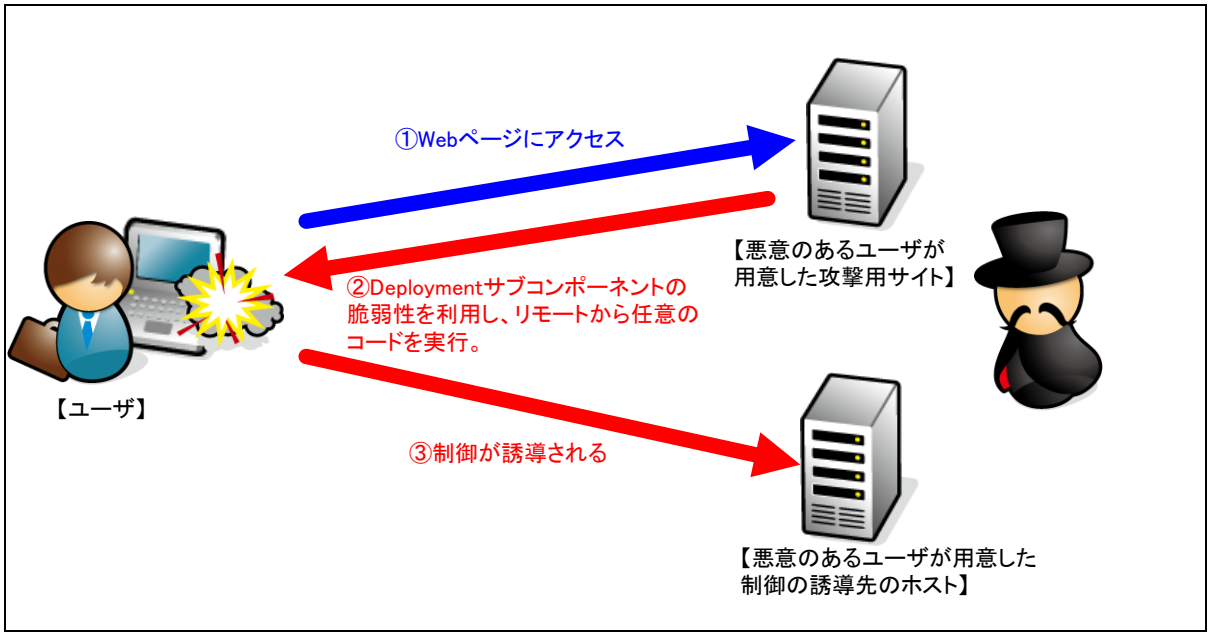
- Oracle Java JDK and JRE 7 Update 3
- Oracle Java JDK and JRE 6 Update 31
- Oracle JavaFX 2.0.3

【参考サイト】

Oracle Java SE Critical Patch Update Advisory - February 2012
http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html

CVE-2012-0500
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-0500

【検証イメージ】



【検証ターゲットシステム】
Windows XP SP3 Internet Explorer 8

【検証概要】
ターゲットシステムに、Web ページを閲覧させ、Java Web Start アプリケーションを開かせることで、攻撃コードを実行させます。それによって、ターゲットシステムにおいて任意のコードを実行させます。
ターゲットシステムは、悪意のあるユーザが用意したホストに制御が誘導されます。

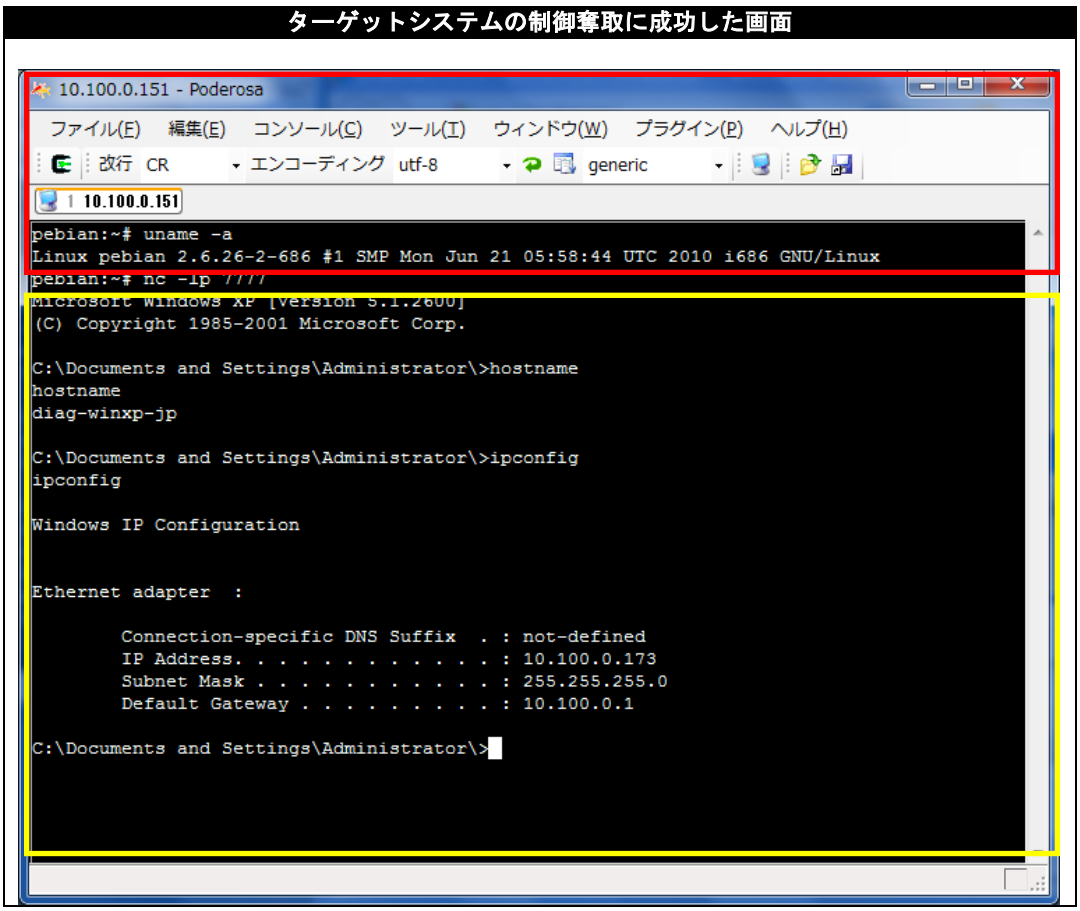
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
＊ 誘導先のシステムは Debian 5.05 です。

NTTデータ先端技術株式会社

【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。

ターゲットシステムの制御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　営業企画グループ
TEL：03-5425-1954
http://security.intellilink.co.jp/