NTTデータ 先端技術株式会社

Oracle Java SE JDK および JRE の脆弱性により、任意のコードが実行される脆弱性 (CVE-2012-1723)に関する検証レポート

2012/7/17
NTT データ先端技術株式会社
辻 伸弘
泉田 幸宏

【概要】

Oracle Java SE JDK および JRE に、リモートより任意のコードが実行される脆弱性が発見されました。本脆弱性は、Java バイトコードを Hotspot VM にて処理を行う際に、コードの検証が不十分であるため、Java のサンドボックスを回避されることにより発生します。

この脆弱性により、リモートから Java を実行するローカルユーザと同じ権限で任意のコードを実行される危険性があります。攻撃者は、ブラウザ経由で Java アプレットを読み込ませるように特別に細工された Web サイトにユーザを誘導することや、細工された Java アプリケーションを添付した電子メールを送信し、攻撃対象ユーザにファイルを開かせることでログオンしているユーザと同じ権限を奪取される危険性があります。

この脆弱性が修正されたバージョンの JDK および JRE が、Oracle 社より 6 月 12 日にリリースされております。しかしながら、攻撃を成立させるためのコードが容易に入手可能であり、かつ脆弱性に対する攻撃が容易であること、また攻撃を受けた際にシステムへの影響が大きいことから、今回、この脆弱性（CVE-2012-1723）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】

- Oracle Java JDK and JRE 7 Update 4 以前
- Oracle Java JDK and JRE 6 Update 32 以前
- Oracle Java JDK and JRE 5 Update 35 以前
- Java SDK and JRE 1.4.2_37 以前

【対策案】

Oracle 社より、この脆弱性を修正するバージョンがリリースされています。
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 5
- Oracle Java JDK and JRE 6 Update 33

※Java SE JDK および JRE のバージョン 6 は、2012 年 11 月でサポート期限が切れます。

【参考サイト】

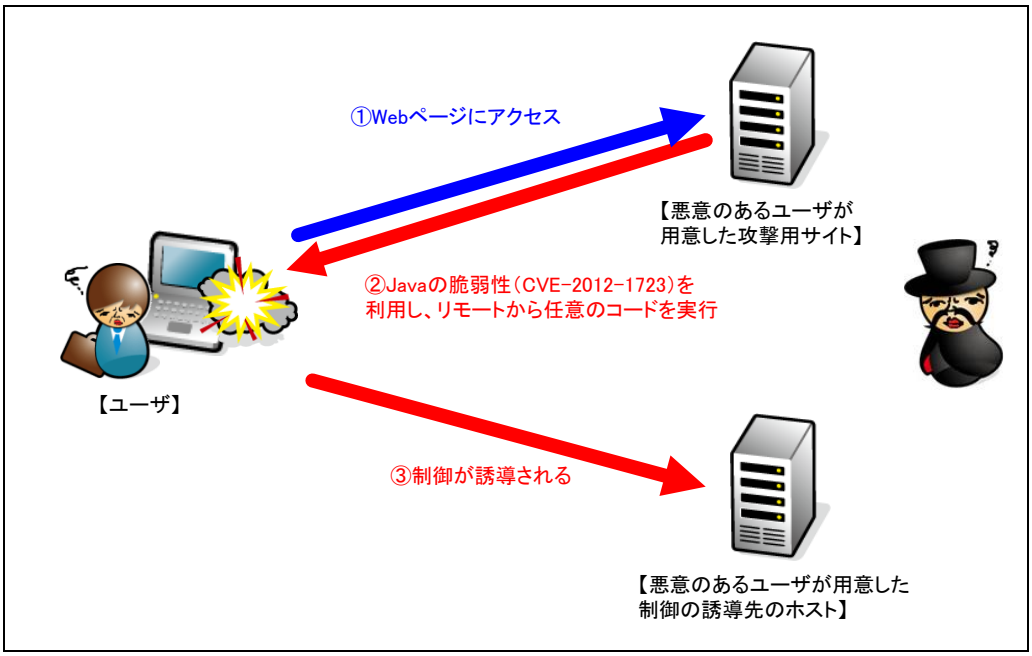
CVE-2012-1723
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723

Oracle Java SE Critical Patch Update Advisory - June 2012
http://www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html

2012 年 6 月 Java SE の脆弱性を狙う攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2012/at120021.html

Oracle Java SE Support Roadmap
http://www.oracle.com/technetwork/java/eol-135779.html

【検証イメージ】



【検証ターゲットシステム】
Windows XP SP3
Java SE JRE 6 Update 32

【検証概要】
ターゲットシステム上で、悪意のあるユーザが作成した Web ページを閲覧させることで、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。

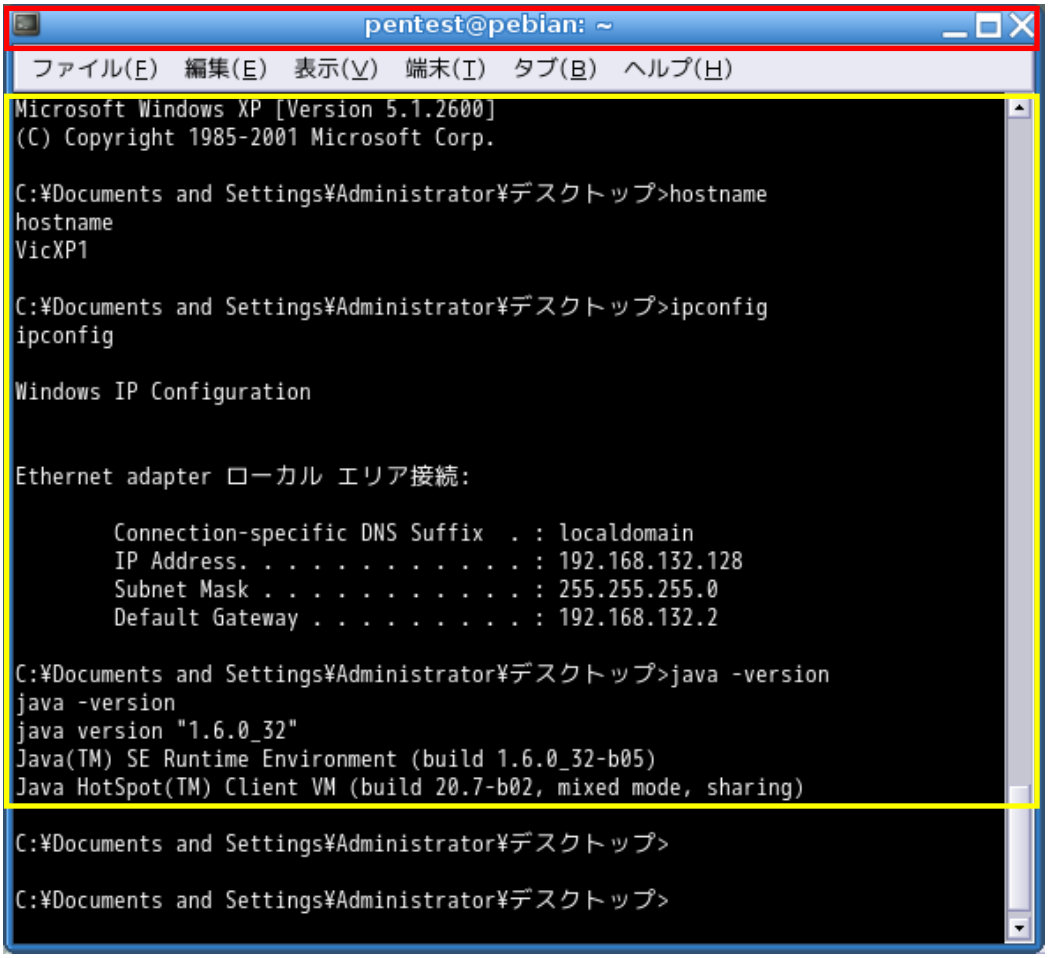
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
＊ 誘導先のシステムは Debian です。

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