NTTデータ 先端技術株式会社

Oracle Java SE JRE の JAX-WS クラスの脆弱性により、任意のコードが実行される脆弱性（CVE-2012-5076）に関する検証レポート

2012/11/14
NTT データ先端技術株式会社
辻 伸弘
泉田 幸宏

【概要】

Oracle Java SE JRE に、リモートより任意のコードを実行される脆弱性が発見されました。
本脆弱性は、JRE の JAX-WS（Java API for XML-Based Web Services）クラスがサンドボックス外の Java コードを実行してしまうことに起因しています。

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 JRE が、Oracle 社より 10 月 16 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-2012-5076）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 7 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 JRE 7 Update 9

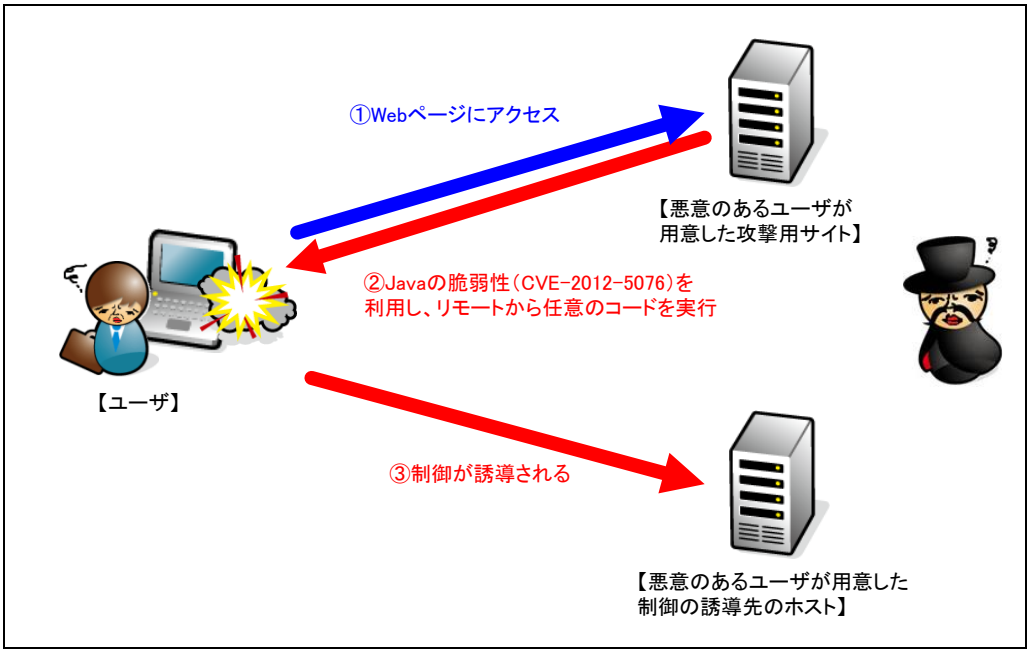
【参考サイト】

CVE-2012-5076
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5076

Oracle Java SE Critical Patch Update Advisory - October 2012
http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html

Oracle Java の脆弱性対策について(CVE-2012-5083 等)
http://www.ipa.go.jp/security/ciadr/vul/20121017-jre.html

【検証イメージ】



【検証ターゲットシステム】
Windows XP, Windows Vista, Windows 8
Java SE JRE 7 Update 7

【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。

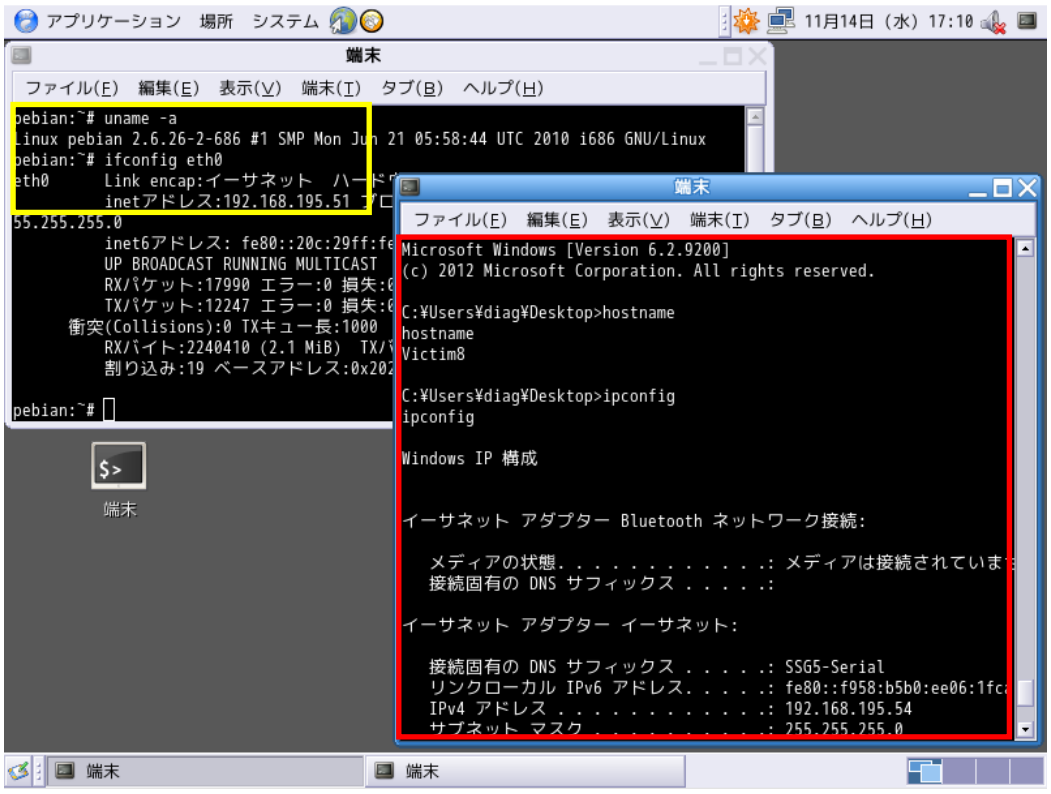
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
＊ 誘導先のシステムは Debian です。

【検証結果】

下図は、攻撃後の誘導先のシステム画面です。

下図は、誘導先のコンピュータ（Debian）の画面です。左上のコンソールの黄線で囲まれている部分は、誘導先のコンピュータのホスト情報および IP アドレスです。一方で、右下のコンソールには、ターゲットシステム（Windows 8）のプロンプトが表示されています。
赤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
TEL：03-5859-5422
http://security.intellilink.co.jp