NTT DATA
NTTデータ 先端技術株式会社

Oracle Java SE JDK および JRE のリフレクション処理の脆弱性により、任意のコードが実行される脆弱性(CVE-2013-2423)に関する検証レポート

2013/4/22
2013/4/26 更新
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を実行される脆弱性が発見されました。本脆弱性は、Java の静的クラスの final フィールドを設定する際、メモリへのアクセス制限が弱いため、リフレクションを利用した際に Type Confusion を引き起こし、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 4 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-2013-2423)の再現性について検証を行いました。

2013 年 4 月 25 日追記：
本脆弱性に対する CVE 番号『CVE-2013-2423』を追記しました。

【影響を受けるとされているシステム】

2013 年 4 月 25 日修正：
- Oracle Java JDK and JRE 7 Update 17 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。
2013 年 4 月 25 日修正：
- Oracle Java JDK and JRE 7 Update 21

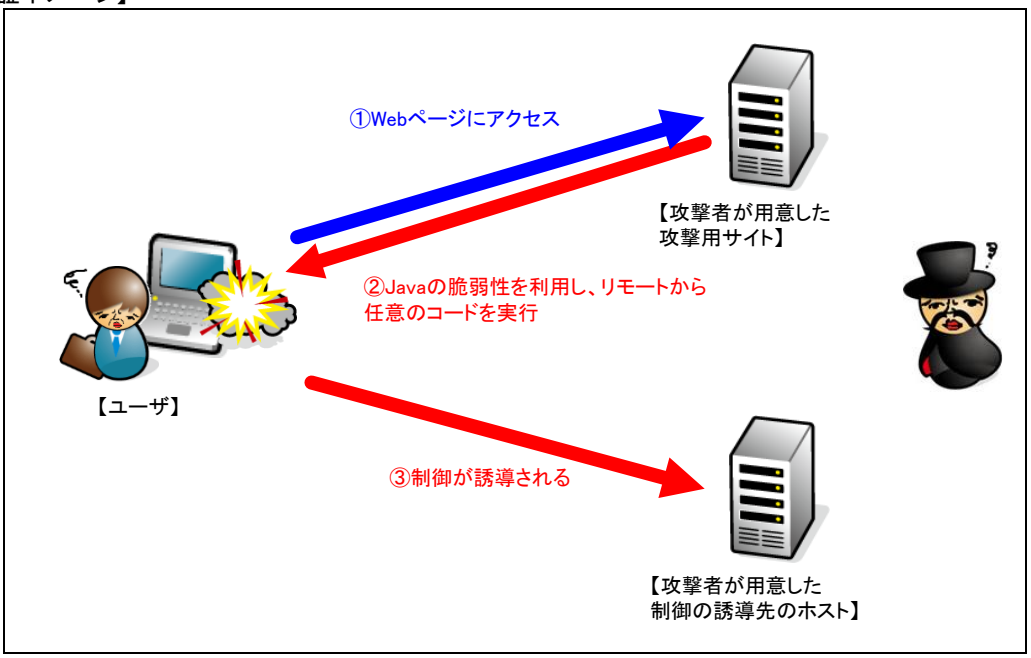
※ 本レポート第一版公開当初 CVE 番号が不明確であったため「影響を受けるとされているシステム」では当該脆弱性を含む「Oracle Java SE Critical Patch Update Advisory - April 2013」で挙げられていた「Affected product releases and versions:」すべてを記載しておりました。しかし、情報が明らかになり当該脆弱性が「CVE-2013-2423」であることが判明したため下記のように情報を更新いたしました。情報が明らかであると判断できない状況であったとはいえ、結果的に不正確な情報となってしまったことをお詫びいたします。

【参考サイト】
Oracle Java SE Critical Patch Update Advisory - April 2013
http://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html

Oracle Java の脆弱性対策について(CVE-2013-2383 等)
https://www.ipa.go.jp/security/ciadr/vul/20130417-jre.html

2013 年 4 月 25 日追記：
CVE-2013-2423
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2423

【検証イメージ】



【検証ターゲットシステム】
Windows XP
Java SE JRE 7 Update 17

【検証概要】
ターゲットシステム上で、攻撃者が作成した 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、攻撃者が用意したホストに制御が誘導されます。

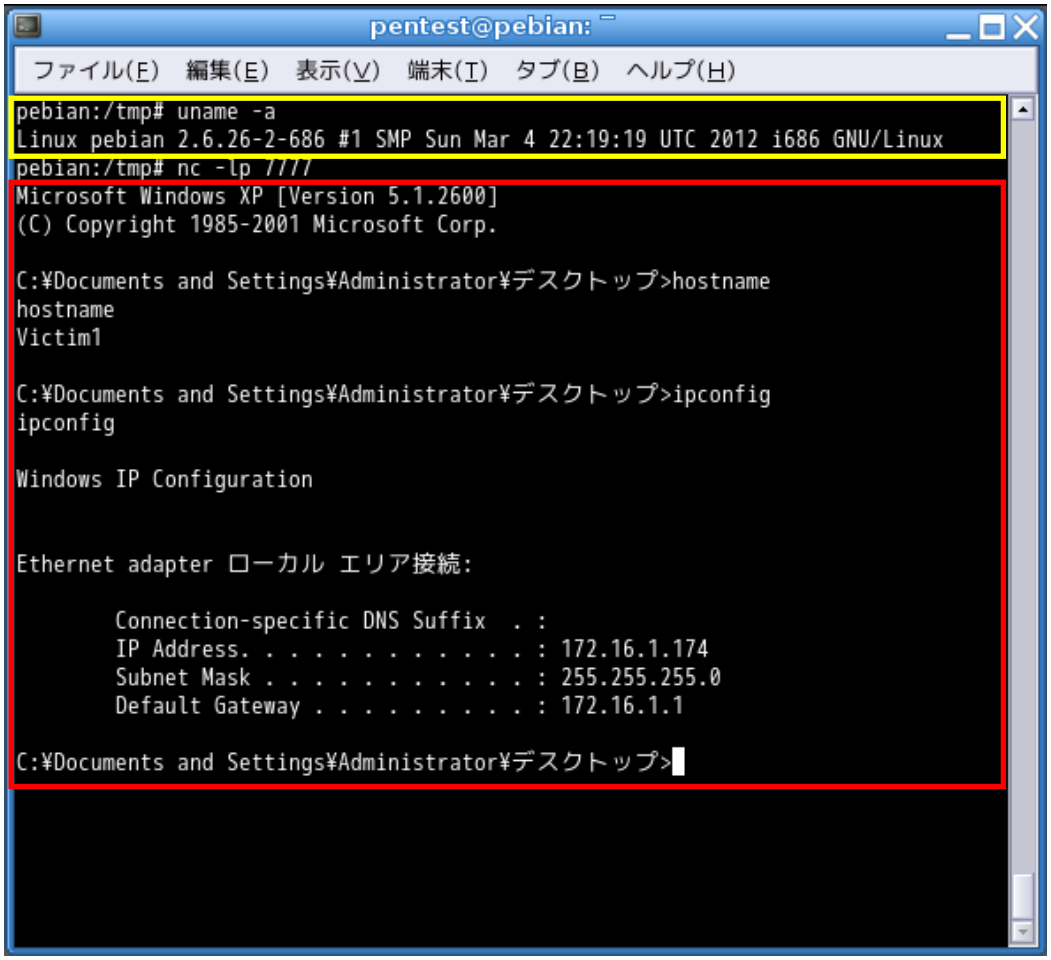
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
＊ 誘導先のシステムは Debian です。

【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。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です。一方で、赤線で囲まれている部分は、ターゲットシステム（Windows XP）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