NTTデータ 先端技術株式会社

Oracle Java SE JDK7 および JRE7 の JMX MBean コンポーネントの脆弱性により任意のコードを実行される脆弱性(CVE-2013-0422)に関する検証レポート

2013/1/11
2013/1/23 更新
NTT データ先端技術株式会社
辻　伸弘
泉田　幸宏
小松　徹也

【概要】

Oracle Java SE JDK7 および JRE7 の Java Management Extensions (JMX) MBean コンポーネントに、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、細工したコードによる JMX MBeanServer クラスのメソッドの利用、および Reflection API の再帰的な利用によるサンドボックス外のコード実行に起因しています。

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。

2013 年 1 月 11 日時点において Oracle 社から脆弱性への対策、回避策などのアナウンスはありません。また、本脆弱性を利用した攻撃そのものが容易でありシステムに与える影響も大きいことから、本脆弱性(CVE-2013-0422)について再現性を検証いたしました。

【影響を受けるとされているシステム】

- Oracle Java JDK および JRE 7 Update 10 以前
(2013 年 1 月 11 日時点)

【対策案】

2013 年 1 月 11 日時点において、Oracle 社から本脆弱性を修正するバージョンはリリースされておりません。攻撃が成立する機会を減らすため、以下の対応が考えられます。

- ウイルス対策ソフトの定義ファイルを最新にする
- 不必要な Web サイトにアクセスしない
- クライアントに余計な通信を許可しない

上記対応は、普段から実施いただくことを推奨いたします。
また、業務等で Java が必要なサイト以外は、一時的に Java プラグインを無効化することも対策となります。

なお、Oracle 社から本脆弱性を修正したバージョンがリリースされた際にはご利用環境への影響を確認の上、アップデートいただくことを推奨いたします。

Java SE ダウンロードサイト
http://www.oracle.com/technetwork/java/javase/downloads/index.html

2013 年 1 月 16 日追記：
Oracle 社から、修正プログラム (Oracle Java JDK and JRE 7 Update 11) がリリースされています。十分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラムの適用を行なうことが推奨されます。
http://www.oracle.com/technetwork/java/javase/7u11-relnotes-1896856.html

修正プログラムを適用した以下のシステムに対して再度検証を行った結果、脆弱性の再現ができないことが確認されました。
・Windows XP SP3 Java SE JRE 7 Update 11

2013 年 1 月 23 日修正：
しかしながら、Oracle 社より提供された今回の修正プログラムのみでは修正されない問題があるとの指摘がセキュリティベンダーよりされております。その指摘内容は、今回のアップデートにより脆弱性 CVE-2013-0422 のうち、Reflection API の問題は修正されているが、JMX MBeanServer への修正は行われていないというものです。このため Reflection API の問題に代わる新たな脆弱性を利用された場合、JMX MBeanServer の問題と組み合わせることにより、本レポートの結果と同じように攻撃の成功に繋がる可能性があります。そのため、引き続き警戒が必要な状態であると判断できます。

Confirmed: Java only fixed one of the two bugs.
http://immunityproducts.blogspot.ca/2013/01/confirmed-java-only-fixed-one-of-two.html

したがって、今後も修正プログラムのリリースの確認を行なうとともに、業務等で必要なサイト以外は Java プラグインを無効化することを推奨いたします。Java プラグインを無効化する方法については各ベンダーより提供されている以下の情報を参考にしてください。

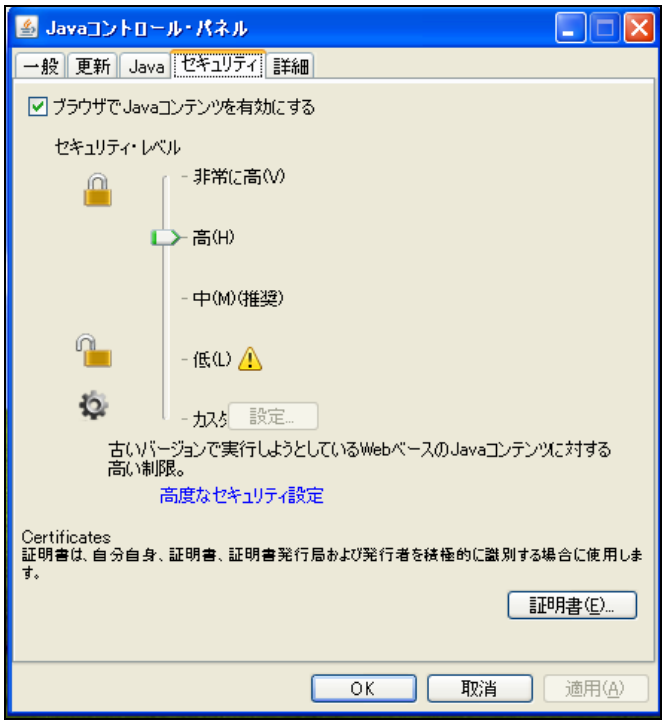
Internet Explorer で Java Web プラグインを無効にする方法
http://support.microsoft.com/kb/2751647/ja

Safari で Java Web プラグインを無効にする方法
http://support.apple.com/kb/HT5241?viewlocale=ja_JP&locale=ja_JP

Java アプレットを無効にするには
https://support.mozilla.org/ja/kb/How%20to%20turn%20off%20Java%20applets

プラグイン
https://support.google.com/chrome/bin/answer.py?hl=ja&answer=142064

また、このアップデートで Java コントロールパネルのセキュリティレベルのデフォルトが「中(M)」から「高(H)」に変更されています。
それによって、無署名の Java アプレットなどを起動しようとすると、必ず警告が表示されます。

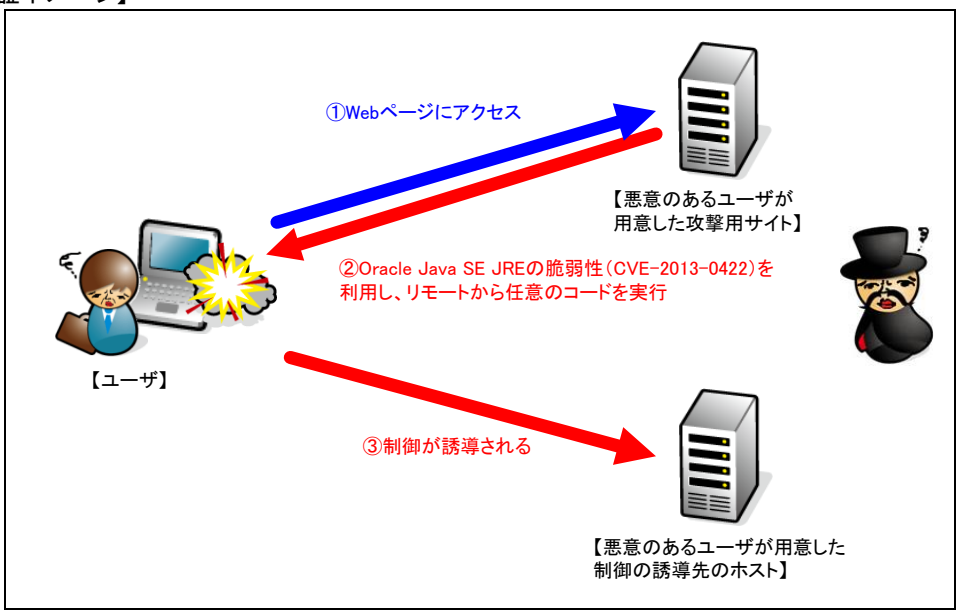


【参考サイト】
CVE-2013-0422
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422

Vulnerability Note VU#625617
http://www.kb.cert.org/vuls/id/625617

2013 年 1 月 16 日追記：
Oracle Security Alert for CVE-2013-0422
http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html

【検証イメージ】



【検証ターゲットシステム】
・Windows XP SP3 Java SE JRE 7 Update 10
・Windows 7 Java SE JRE 7 Update 10

【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。

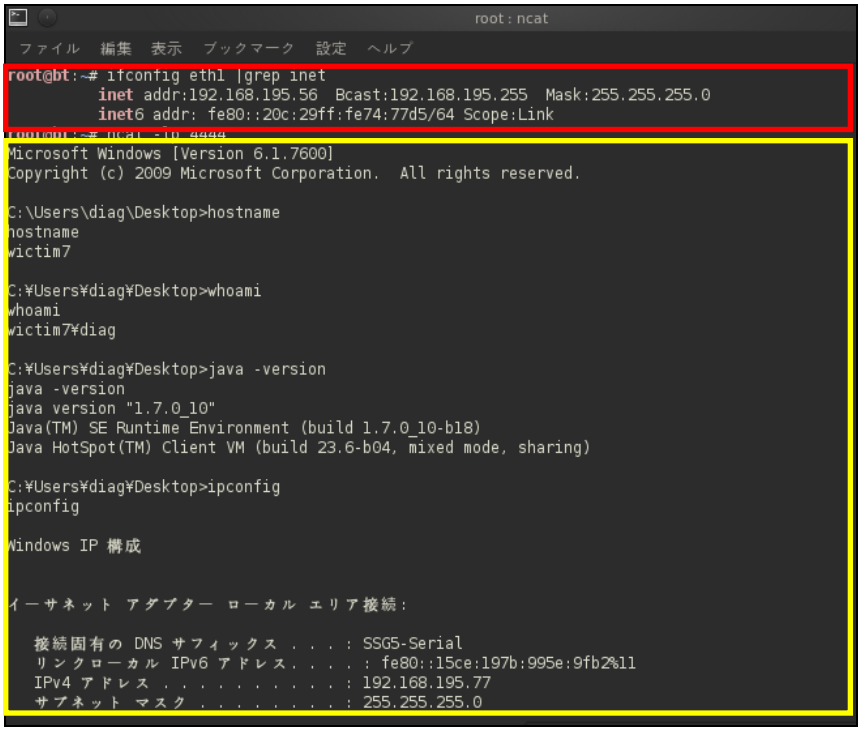
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
＊ 誘導先のシステムは Ubuntu 10 です。

【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（Ubuntu 10）のターミナル上にターゲットシステム（Windows 7）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
TEL： 03-5859-5422
http://security.intellilink.co.jp