NTT DATA
NTTデータ 先端技術株式会社

Oracle Java SE JDK7 および JRE7 の MethodHandle 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-2012-5088)に関する検証レポート

2013/1/28
NTT データ先端技術株式会社
辻　伸弘
小田切　秀暁

【概要】

Oracle Java SE JDK7 および JRE7 の MethodHandle 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。MethodHandle 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が、Oracle 社より 2012 年 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、本脆弱性（CVE-2012-5088）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 および 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 11

なお、Oracle 社より提供された上記の最新版でも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。詳細は、以下の検証レポートを参照ください。

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
http://security.intellilink.co.jp/article/vulner/130111.html

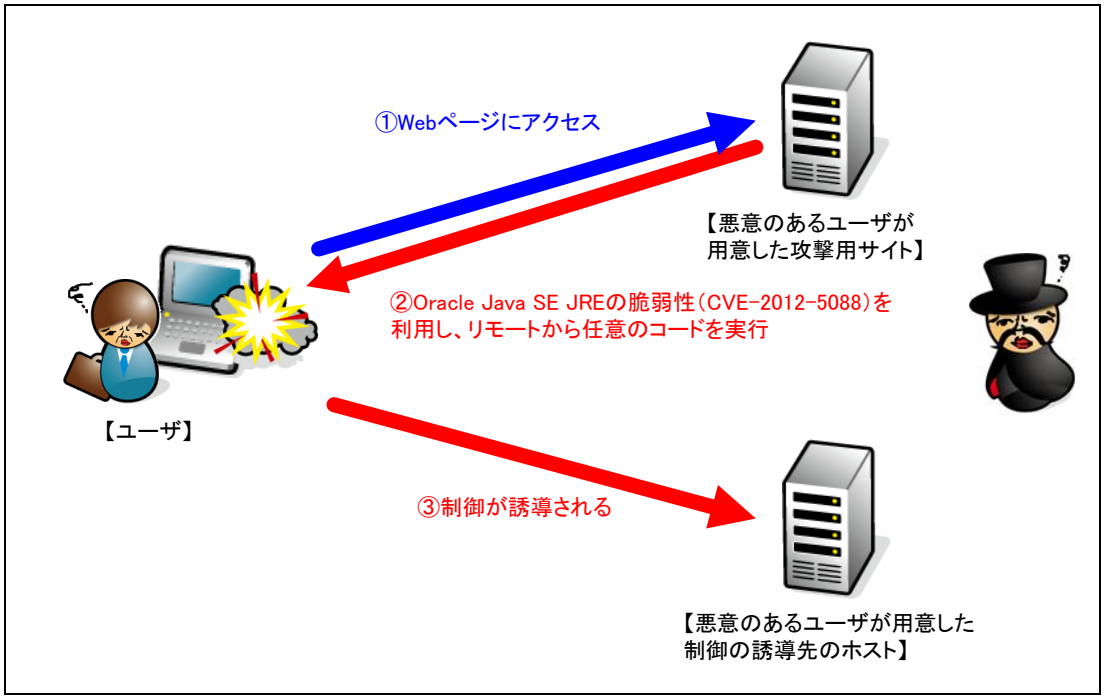
【参考サイト】

CVE-2012-5088
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5088

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 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 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 Thu Nov 3 04:23:54 UTC 2011 i686 GNU/Linux
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>
C:\Users\diag\Desktop>hostname
hostname
Victim8

C:\Users\diag\Desktop>java -version
java -version
java version "1.7.0_07"
Java(TM) SE Runtime Environment (build 1.7.0_07-b10)
Java HotSpot(TM) Client VM (build 23.3-b01, mixed mode, sharing)

C:\Users\diag\Desktop>ipconfig
ipconfig

Windows IP 構成


イーサネット アダプター Bluetooth ネットワーク接続:

   メディアの状態. . . . . .: メディアは接続されていません
   接続固有の DNS サフィックス . . . . .:

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 . . . . .: localdomain
   リンクローカル IPv6 アドレス. . . . .: fe80::f958:b5b0:ee06:1fca%12
   IPv4 アドレス . . . . . .: 192.168.14.132
   サブネット マスク . . . . . .: 255.255.255.0
   デフォルト ゲートウェイ . . . . . .: 192.168.14.2
```

＊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