株式会社 日立システムズ

SSRC-VR-20130507

発行日:2013/05/07

S.S.R.C.

脆弱性検証レポート

(CVE-2013-2431)

株式会社　日立システムズ

セキュリティリサーチセンタ

S.S.R.C.脆弱性検証レポート

目次

1. はじめに

S.S.R.C.(Shield Security Research Center)は、株式会社日立システムズ　セキュリティリサーチセンタが運営するセキュリティ情報公開サイトです。本サイトでは、セキュリティリサーチセンタによるリサーチ結果を随時配信する予定です。

本文書は、株式会社日立システムズ、SHIELD セキュリティセンタで日々収集を行っている世界中のセキュリティトレンド情報にもとづき、セキュリティリサーチセンタのセキュリティアナリストが確認した、ソフトウェア等の脆弱性検証結果をまとめたレポートです。

次に示す、ご利用条件を十分にお読み頂き、ご了承頂いた上でご利用頂きます様、よろしくお願い致します。

2. ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）と致しましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。

本文書に掲載されている情報は、掲載した時点での情報です。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。

3. 概要

3.1. 脆弱性の概要

Oracle 社が提供する Java 7 には、任意のコードが実行可能な脆弱性 CVE-2013-2431 (以降、本脆弱性)が存在します。

悪意のあるウェブサイトを閲覧したりすることで、Java のサンドボックスを回避され、任意のコードを実行されてしまう可能性があります。その結果、ログインしているユーザ権限で、コンピュータを操作されてしまいます。

3.2. 影響を受けるシステム

- JDK 7 Update 17 およびそれ以前
- JRE 7 Update 17 およびそれ以前

3.3. 深刻度

深刻度:危険

CVSS 基本値:10.0 [SSRC 評価]

3.4. 対策方法

- **根本的対策**

Oracle 社より、本脆弱性に対応したアップデート版が公開されています。下記の URL より、至急アップデートを実施してください。

http://java.com/ja/download/ (Oracle 社)

なお、Java が不要な場合、アンインストールしておくことも有効な対策となります。

- **緩和策**

下記の情報をもとに、ブラウザ上での Java プラグインの実行を無効にするか、自動実行を抑制してください。

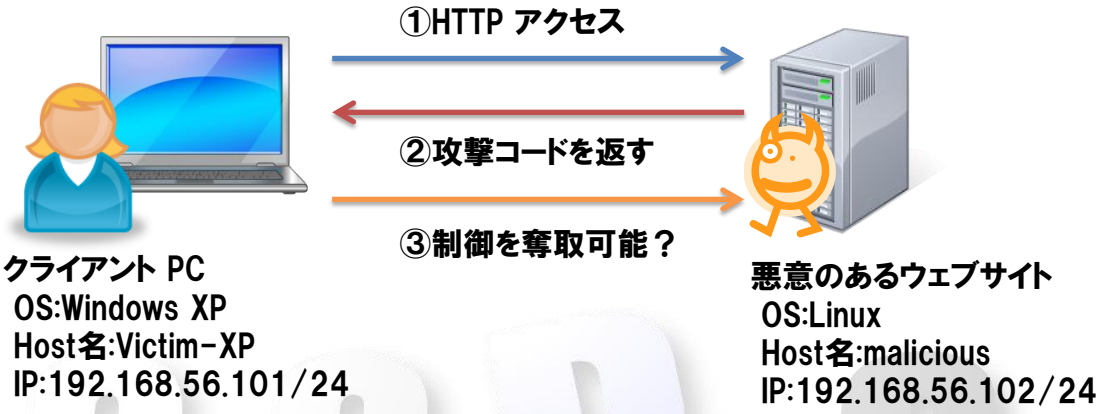
- Internet Explorer
  http://support.microsoft.com/kb/2751647/ja
- Firefox
  https://support.mozilla.org/ja/kb/How%20to%20turn%20off%20Java%20applets
- Google Chrome
  https://support.google.com/chrome/bin/answer.py?hl=ja&answer=142064

なお、詳細な手順は「S.S.R.C.テクニカルレポート～ブラウザプラグインのセキュリティ設定編～」にも記載しております。

http://www.shield.ne.jp/ssrc/doc/SSRC-TER-20130226.pdf

4. 検証

本検証のイメージは下記のとおりです。Windows XP クライアントから、悪意のあるウェブサイトに見立てた Linux サーバに HTTP アクセスを行い、Linux サーバ上から Windows XP を制御することが可能か検証します。本検証では、一般に公開されているいくつかの情報源から集めた検証コードを、独自にカスタマイズした上で検証を行いました。



4.1. 脆弱なバージョンの JAVA を利用した検証

- **検証環境**

  クライアント：

  OS　　：Windows XP SP3 日本語版(2013/01/15 時点での最新パッチ適用済み)

  Java　　：1.70_17

- **検証結果**

  図 1 は、クアイアント PC から、Linux サーバへアクセスした際の画面です。ブラウザ上では、悪意のある Java Applet が動作しています。このようなウェブページにブラウザでアクセスしてしまうと、クライアント PC の制御を奪われてしまいます。

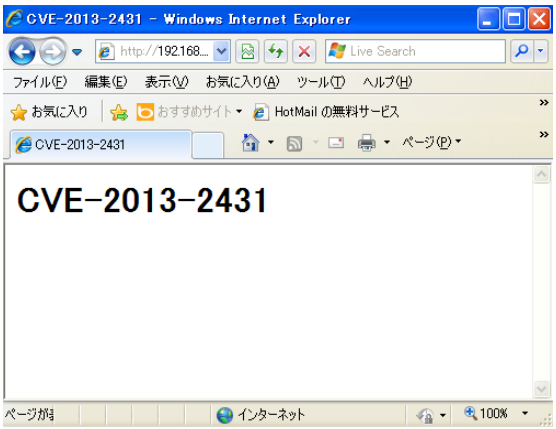


図 1 クライアント PC から、検証コードが設置されたページにアクセスした画面

図 2 は、Linux サーバ上でのターミナルの画面です。本脆弱性を悪用することで、クライアント PC を制御出来ていることがわかります。

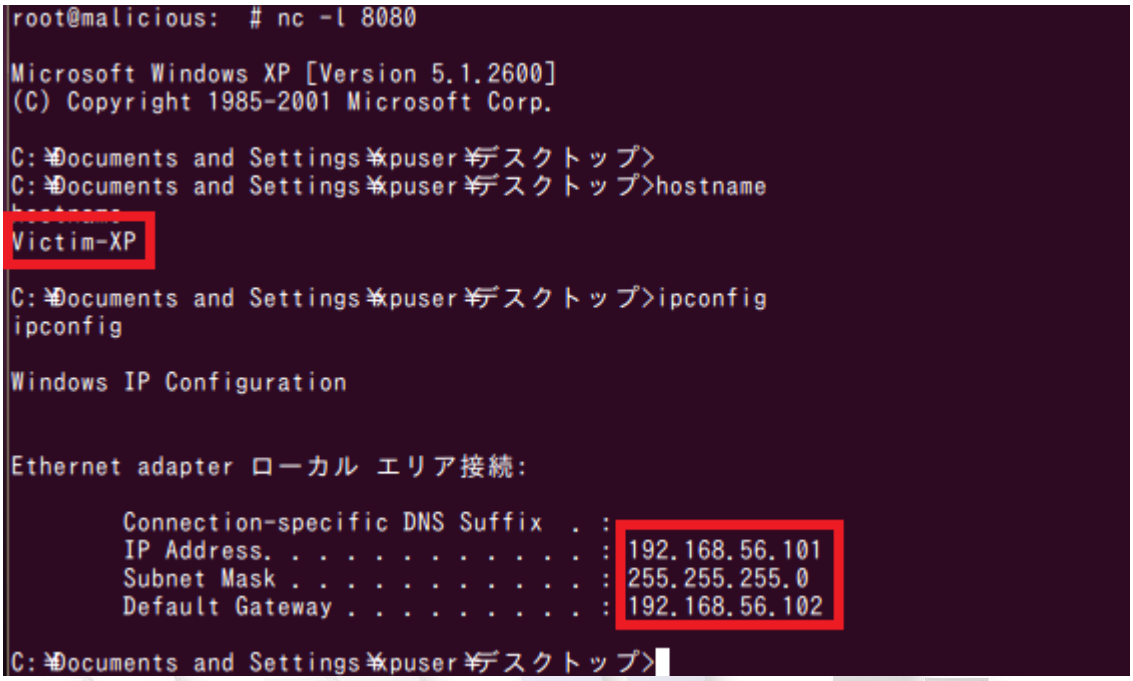


図 2 クライアント PC の制御を奪った画面

4.2. 修正済みバージョンの JAVA を利用した検証

- **検証環境**

  OS　　: Windows XP SP3 日本語版(2013/04/24 時点での最新パッチ適用済み)
  Java　　: 1.70_21

- **検証結果**

  「4.1 脆弱なバージョンの JAVA を利用した検証」と同様の手順で検証を実施しましたが、Linux サーバから、クライアント PC 制御は出来ませんでした。

4.3. Windows7 における検証

- **検証環境**

  OS　　: Windows 7 SP1 日本語版(2013/04/24 時点での最新パッチ適用済み)
  Java　　: 1.70_17

- **検証結果**

  Windows XP を利用した検証と同様に、Linux サーバから、クライアント PC(Windows 7)の制御を奪うことが可能でした。

5. まとめ

Java (1.7.0_17)を利用した検証では、現時点で公開されている検証コードを用いることで、制御が奪われましたが、本脆弱性の修正済みバージョンとされている Java (1.7.0_21)を利用した検証では、制御を奪われることがないことを確認しました。

しかし、Java (1.7.0_21)で修正された脆弱性の対策は一部にのみ有効であり、まだ脆弱性が残存しているとの情報がございます。

そのため、事前対応策として、アップデートの実施と共に、3.4 で紹介した緩和策(Java プラグインの実行無効化、自動実行の抑制)の実施を推奨します。

[参考文献]

- ベンダ情報

(i). http://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html

- その他情報

(ii). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2431

(iii). http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2431

(iv). http://jvn.jp/cert/JVNTA13-107A/index.html

(v). http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-002386.html

S.S.R.C.

Shield Security Research Center

株式会社　日立システムズ
〒141-8672 東京都品川区大崎 1-2-1
http://www.hitachi-systems.com/index.html
http://www.shield.ne.jp/ssrc/index.html