

「Java Web Start」におけるセキュリティ上の弱点(脆弱性)の注意喚起

独立行政法人 情報処理推進機構(略称:IPA、理事長:藤原武平太)は、「Java Web Start」におけるセキュリティ上の弱点(脆弱性)に関する注意喚起を本日公表しました。

(URL: http://www.ipa.go.jp/security/vuln/200705_JWS.html)

具体的には、ウェブブラウザ上で悪意あるリンクをクリックした場合などに、リモートから任意のコードを送り込まれ、実行されるというものです。悪用されると、利用者のコンピュータ内の情報が漏えいしたり、改ざんされたりする可能性があります。

対策方法は「ベンダが提供する対策済みバージョンに更新する」ことです。

1. 概要

一般に、インターネット利用者がウェブブラウザなどで Java アプリケーションを動作させる場合、Java アプリケーションの実行環境を提供するソフトウェアが必要となります。そのようなソフトウェアの一つとして、サン・マイクロシステムズ社が配布している JRE (Java Runtime Environment) があります。

Java Web Start は、JRE などに同梱されているソフトウェアです。JRE をインストールした場合や、JDK (Java Development Kit) などの JRE を含むソフトウェアをインストールした場合、同時にインストールされます。

Java Web Start の機能により、ウェブブラウザ上などから Java アプリケーションを起動できるようになります。このとき Java アプリケーションは、利用者のコンピュータ内の情報を読み書きすることができない、いわゆるサンドボックス機構の中で動作します。これにより、もし Java アプリケーションに悪意あるコードが含まれていた場合でも、利用者のコンピュータは保護されます。

しかし、Java Web Start の実装に問題があるため、本来実行が許可されていないシステムクラス¹が実行される可能性があります。システムクラスは、サンドボックスの制限を受けないため、本問題により悪意あるコードが利用者のコンピュータで実行される可能性があります。悪用されると、利用者のコンピュータ内の情報が漏えいしたり、改ざんされたりする可能性があります。

最新情報は、次の URL を参照して下さい。

http://www.ipa.go.jp/security/vuln/documents/2007/JVN_44724673.html

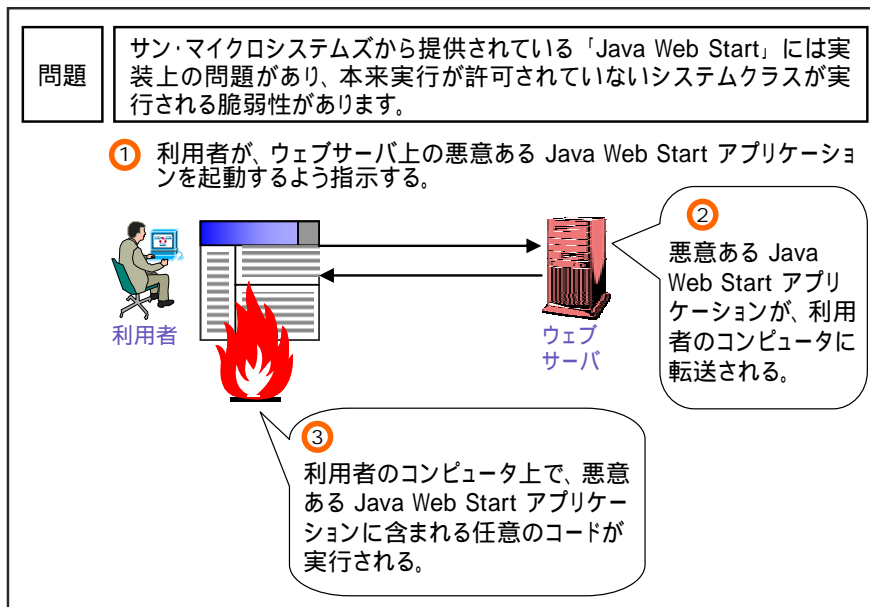


図 1 「Java Web Start」において許可されていないシステムクラスが実行される脆弱性

2. セキュリティ上の弱点による影響

利用者のコンピュータで、悪意あるコードが実行される可能性があります。その結果、利用者のコンピュータ内の情報が漏えいしたり、改ざんされたりする可能性があります。

¹ Java において、JRE に同梱されているクラス。システムクラスは、信用することのできないプログラムを、安全に実行するためのセキュリティモデルであるサンドボックスの制限を受けずに動作することができる。

3. 対策方法

対策方法は「ベンダが提供する対策済みバージョンに更新する」ことです。

なお、JRE をバージョンが異なるものに更新した場合、一部の Java アプリケーションの動作に支障をきたす場合があります。各 Java アプリケーションの動作環境を確認の上、対策を行ってください。

3.1 対策済みバージョン(update 版)に更新する方法

JVN 脆弱性対策情報「JVN#44724673 Java Web Start において許可されていないシステムクラスが実行される脆弱性(URL: <http://jvn.jp/jp/JVN%2344724673/index.html>)」のベンダ情報欄を参照下さい。

要約すると、次のサン・マイクロシステムズ社ページに記載された「2. Contributing Factors」の方法で影響を受けるシステムが否かを判断し、「5. Resolution」の方法で対策済みバージョン(update 版)に更新して下さい。

Sun Alert #102881 Security Vulnerability With Java Web Start Related to Incorrect Use of System Classes
(URL: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-102881-1>)

更新後、古いバージョンの JRE があるかを確認し、古いバージョンの JRE があれば削除して下さい。古いバージョンの削除要否については、表 1 を参照して下さい。

表 1. 対策済みバージョン導入後の古いバージョンの削除要否

導入した対策済みバージョン	古いバージョンの削除要否
JRE 5.0 最新版のみ	不要
JRE 1.4.2 最新版のみ	要
JRE 1.4.2 最新版と JRE 5.0 最新版の両方	不要
JRE 1.4.2 最新版と JRE 6 最新版の両方	不要

本注意喚起は、JRE に同梱されている「Java Web Start」の脆弱性に関するものですが、JRE は 2007 年 7 月 25 日時点で、本件とは別の新たな脆弱性が修正されています。JRE 5.0 または JRE 6 の最新版を導入していない場合は古いバージョンの削除が必要です。

例 1) Windows で JRE 5.0 Update 10 およびそれ以前を使用している場合

次のサン・マイクロシステムズ社ページより、update 版をダウンロードしてインストールします。

<http://java.sun.com/j2se/1.5.0/download.jsp>

(1) Java Runtime Environment (JRE) 5.0 Update 12 の「Download」ボタンをクリック。

(2) Accept License Agreement のラジオボタンをクリック。

(3) Windows Platform - Java Runtime Environment 5.0 Update 12 の下にある、

Windows Offline Installation, Multi-language をクリック後、指示に従いインストールする。

例 2) Windows で JRE 1.4.2 Update 13 およびそれ以前を使用している場合

次のサン・マイクロシステムズ社ページより、update 版をダウンロードしてインストールします。インストール後、古いバージョンの JRE があれば削除します。

<http://java.sun.com/j2se/1.4.2/download.html>

(1) J2SE v 1.4.2_15 JRE includes the JVM technology の「Download J2SE JRE」をクリック。

(2) Accept License Agreement のラジオボタンをクリック。

(3) Windows Platform - Java(TM) 2 Runtime Environment, Standard Edition 1.4.2_15 の下にある、

Windows Offline Installation, Multi-language をクリック後、指示に従いインストールする。

(4) コントロールパネルの「プログラムの追加と削除」を開き、1.4.2_15 より古い JRE があるか確認する。

(5) 1.4.2_15 より古い JRE があれば「プログラムの追加と削除」から削除する。

3.2 Windows で Java Update を利用して更新する方法

次のサン・マイクロシステムズ社ページ「Java Update とは何ですか」を参照し、更新して下さい。

<http://www.java.com/ja/download/help/5000020700.xml>

なお、この方法では、JRE が最新のバージョンに更新されます(2007/7/25 現在、JRE バージョン 6)。使用中の JRE をバージョンが異なるものに更新した場合、一部の Java アプリケーションの動作に支障をきたす場合があります。その場合は、3.1 の方法で更新を行ってください。

本内容に関するお問い合わせ先

独立行政法人 情報処理推進機構 セキュリティセンター(IPA/ISEC)
Tel:03-5978-7527 Fax:03-5978-7518 E-mail: vuln-inq@ipa.go.jp