

Java VM Vulnerability

分類 トロイの木馬/なりすまし
再現性 リモート

技術解説

1) 概要

Microsoft VM (Microsoft Virtual Machine) を実装しているクライアントが、悪意ある Web サーバに接続すると、Java アプレットのセキュリティ仕様を回避できるという脆弱性をついた Java アプレットが実行される可能性がある。これにより、クライアントのローカルファイル・レジストリの書き換えや、クライアントと信頼関係のあるサーバの情報が悪意ある Web サーバに取得される可能性がある。

2) 原因

Java アプレットは、あるサイトを参照した際に自動的にダウンロードされ、実行されるという特徴をもつため、その実行にはセキュリティ上の制限がかけられている。ダウンロードされた Java アプレットコードは、リモートからロードされたコードと、ローカルからロードされたコードに分けて取り扱われ、リモートからロードされたコードに対しては、実行に際してより厳しいセキュリティ制限がかけられている。原則としてリモートからダウンロードされたコードは、ローカルディスクにはアクセスできず、ダウンロードした Web サーバ以外のサーバに対しては TCP/IP 通信ができない仕様となっている。ローカルディスクへのアクセス、ダウンロードした以外のサーバへの TCP/IP 通信を行うためには、コードに署名がされている必要がある。

しかし、Microsoft VM には、ローカルディスクへアクセスするオブジェクトが挿入されているアプレットコードを、セキュリティ上安全なローカルコードとして取り扱ってしまう場合がある。これにより署名がないコードでもローカルディスクへのアクセス、ダウンロードしたサーバ以外のサーバに対しての TCP/IP 通信が可能となる。

ActiveX コンポーネントの1つである、com.ms.ActiveX が挿入されているアプレットコードは、これに該当する。

Java アプレットの SandBox セキュリティモデルに関する参考URL

<http://hata.cc/docs/SignedObj/Why.html>

<http://java.sun.com/j2se/1.3/ja/docs/ja/guide/security/spec/security-spec.doc1.html#21150>

http://www.tetras.co.jp/yada/j_websec_r.htm

<http://hata.cc/docs/SignedObj/Points.html>

影響

Microsoft VM を実装しているクライアントが、悪意ある Web サーバに訪問すると、署名なしの Java アプレットコードをダウンロードし、“SandBox”外で実行してしまう可能性がある。この Java アプレットが実行されることにより、クライアントのローカルディスクへのアクセス、Java アプレットをダウンロードした以外の任意のホストとの TCP/IP 通信が行われる可能性がある。

この脆弱性を利用し、クライアントのローカルファイルやレジストリの書き換えが行われる可能性がある。また、クライアントより張られた悪意ある Web サーバとのセッションを利用し、悪意ある Web サーバが、クライアントを中継として、クライアントと信頼関係にある他のサーバの情報を取得する可能性がある。このサーバがイントラネット上でしか公開されていない Web サーバである場合や、クライアントが利用するオンラインバンクへのユーザ ID/パスワードがキャッシュに残っている場合など、機密情報や個人情報が漏洩する可能性がある。

影響を受けるOS、サービス

影響 ○:脆弱性あり、×:脆弱性なし

(2001/6/26現在)

OS	アプリケーション	バージョン(ビルド番号)	影響	備考
全ての Windows	Microsoft JavaVM	2000-2445	○	
		3000-3194	○	
		3229-3240	○	
		3300-3313	○	
		上記以外	×	

参考 URL

[Microsoft US]

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-059.asp>
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq00-059.asp>
<http://www.microsoft.com/technet/support/kb.asp?ID=271752>

[Microsoft Japan]

http://www.microsoft.com/japan/technet/security/prekb.asp?sec_cd=MS00-059
http://www.microsoft.com/japan/technet/security/SecFAQ.asp?sec_cd=ms00-059
<http://www.microsoft.com/JAPAN/support/kb/articles/JP271/7/52.htm>

OS 全ての Windows
 アプリケーション Microsoft VM 2000-2445,3000-3194,3229-3240,3300-3313

対策方法

1)対策

この問題が対策済みである、build 3802(2001年1月25日リリース)以上にバージョンアップする。

[英語版の場合]

ダウンロード先:

http://www.microsoft.com/java/vm/dl_vm40.htm**[日本語版の場合]**

ダウンロード先:

http://www.microsoft.com/japan/java/vm/dl_vm40.asp**2) Advisory情報****Microsoft Security Bulletin MS00-059(US):**<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-059.asp><http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq00-059.asp><http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq00-059.asp><http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq00-059.asp>**Microsoft Support Knowledge Base Article Q271752(US):**<http://support.microsoft.com/support/kb/articles/q271/7/52.asp?id=271752&sd=tech>**Microsoft Security Bulletin MS00-059(Japan):**http://www.microsoft.com/japan/technet/security/prekb.asp?sec_cd=MS00-059http://www.microsoft.com/japan/technet/security/SecFaq.asp?sec_cd=ms00-059**Microsoft Support Knowledge Base Article JP271752:**<http://www.microsoft.com/JAPAN/support/kb/articles/JP271/7/52.htm>