

Microsoft Internet Explorer Javaprxy.DLL COM Object Instantiation Heap Overflow Vulnerability

分類 Buffer Overflow/受動的攻撃
再現性 リモート

技術解説

1)概要

Microsoft Internet Explorer (以下「IE」という。)には、object タグを利用して javaprxy.dll を呼び出すような HTML ファイルを参照した際にバッファオーバーフローを引き起こす問題がある。リモートの攻撃者により、Web ページや電子メールを介して、この問題が悪用された Web ページを参照させられることで、参照したユーザの権限で任意のコードが実行される可能性がある。

なお、この問題は Microsoft Security Bulletin MS05-037 として公開されているものである。

対策方法

1)対策

Windows Update を利用することにより、マイクロソフト社から提供されている修正プログラム (903235) を適用する。また、Windows Update を利用しない場合は、下記の参考サイトなどを参考にして、個別に修正プログラムを入手し適用する。

また、以下に示す対策のいずれかを行うことで、この問題を回避することが可能である。

- レジストリを変更することにより COM オブジェクトを無効にする。
- Internet Explorer のセキュリティ設定で、ゾーンの設定を「高」に設定する。
- Internet Explorer のセキュリティ設定で [ActiveX コントロールとプラグインの実行] を [ダイアログを表示する] または [無効にする] に設定する。
- 下記のコマンドを実行することで、COM オブジェクトの登録を解除する。

```
regsvr32 /u javaprxy.dll
```

- 下記のコマンドを実行することで、Javaprxy.dll のアクセス制御リストの制限を厳しくする。

```
cacls %windir%\system32\javaprxy.dll /d everyone
```

- レジストリを編集する事で、ソフトウェア制限ポリシーを使用して、Internet Explorer の Javaprxy.dll へのアクセスを制限する (Windows XP 以降のバージョンの Internet Explorer)
- Microsoft JVM の削除ツールを使用してシステムから Microsoft Java Virtual Machine を削除する

参考サイト:

2) Advisory情報

Microsoft Security Bulletin MS05-037 (英語版):

<http://www.microsoft.com/technet/security/Bulletin/MS05-037.msp>

Microsoft Security Bulletin MS05-037 (日本語版):

<http://www.microsoft.com/japan/technet/security/Bulletin/MS05-037.msp>

Microsoft Security Advisory (903144) (英語版):

<http://www.microsoft.com/technet/security/advisory/903144.msp>

Microsoft Security Advisory (903144) (日本語版):

<http://www.microsoft.com/japan/technet/security/advisory/903144.msp>

Vulnerability Note VU#939605:

<http://www.kb.cert.org/vuls/id/939605>

FrSIRT/ADV-2005-0935:

<http://www.frstirt.com/english/advisories/2005/0935>

SecurityFocus BID 14087:

<http://www.securityfocus.com/bid/14087>

検証有無

結果 ○:成功、×:失敗、-:未検証

OS	アプリケーション	バージョン	結果
Windows 2000 Advanced Server SP4 (J)	Internet Explorer	6.0 SP1	○
Windows 2000 Advanced Server SP4 (E)			○
上記以外の組み合わせ			-

検証結果

1) 検証環境

	OS	サービス/アプリケーション	備考
攻撃側	Windows 2000 Advanced Server SP4 (J)	IIS 5.0	
ターゲット	Windows 2000 Advanced Server SP4 (J)	Internet Explorer 6.0 SP1	

痕跡

1) ログ

ターゲットホストのイベントログ (アプリケーション) に、以下のログが出力される。

```
イベントの種類: エラー  
イベント ソース: Microsoft Internet Explorer  
イベント カテゴリ: なし
```

イベント ID: 1000

日付: 2005/07/07

時刻: 16:37:53

ユーザー: N/A

コンピュータ: HOST01

説明:

イベント ID (1000) (ソース Microsoft Internet Explorer 内) に関する説明が見つかりませんでした。リモート コンピュータからメッセージを表示するために必要なレジストリ情報またはメッセージ DLL ファイルがローカル コンピュータにない可能性があります。次の情報はイベントの一部です: iexplore.exe, 6.0.2800.1106, javaprx.dll, 5.0.3810.0, 00008666.

データ:

0000: 41 70 70 6c 69 63 61 74 Applicat

0008: 69 6f 6e 20 46 61 69 6c ion Fail

0010: 75 72 65 20 20 69 65 78 ure iex

0018: 70 6c 6f 72 65 2e 65 78 plore.ex

0020: 65 20 36 2e 30 2e 32 38 e 6.0.28

0028: 30 30 2e 31 31 30 36 20 00.1106

0030: 69 6e 20 6a 61 76 61 70 in javap

0038: 72 78 79 2e 64 6c 6c 20 rxy.dll

0040: 35 2e 30 2e 33 38 31 30 5.0.3810

0048: 2e 30 20 61 74 20 6f 66 .0 at of

0050: 66 73 65 74 20 30 30 30 fset 000

0058: 30 38 36 36 36 0d 0a 08666..

また、ターゲットホストのイベントログ (システム) に、以下のログが出力される。

イベントの種類: 情報

イベント ソース: Application Popup

イベント カテゴリ: なし

イベント ID: 26

日付: 2005/07/07

時刻: 16:40:20

ユーザー: N/A

コンピュータ: HOST01

説明:

アプリケーション ポップアップ: IEXPLORE.EXE - アプリケーション エラー :
"0x7c508666" の命令が "0x0000ff64" のメモリを参照しました。メモリが "read" になることはできませんでした。

プログラムを終了するには [OK] をクリックしてください

プログラムをデバッグするには [キャンセル] をクリックしてください

2) 痕跡

Temporary Internet Files フォルダに、参照した HTML ファイルが残った。