

IE Arbitrary Program Execution Vulnerability

分類 Access Validation Error / 受動的攻撃
関連ツール名称
再現性 リモート

技術解説

1) 概要

Microsoft Internet Explorer には、悪意あるスクリプトを含む Web サイト、もしくは電子メールを閲覧した場合、攻撃者に任意のプログラムを実行されてしまう問題がある。また、この問題は 2000 年 6 月 24 日に、SecurityFocus などで公開された Force Feeding 問題が関連していると推測される。

2) 原因

今回の問題と深い関連があると推測される Force Feeding 問題は、CLASSID に、オールゼロ以外の適当な ID を指定し、CODEBASE パラメータ(※1)にターゲットホスト上の任意のプログラムのパスを指定することで、ターゲットホスト上の任意のプログラムを実行するという問題であった。その後、リリースされた Internet Explorer では、Force Feeding の手法を利用した問題は修正されていたが、根本的な問題の修正がなされていなかったものと思われ、今回の問題は、window.createPopup() もしくは、window.open() などで作成した新しいオブジェクトを利用することで、Force Feeding 問題と同様の問題が発生するものである。

ActiveX コントロールを識別する ID である CLASSID に、オールゼロ以外の適当な ID を指定し、CODEBASE パラメータに任意のプログラムのパスを指定したものを、window.createPopup() もしくは、window.open() で作成した新しいオブジェクトに渡すことで、CODEBASE パラメータに指定されたプログラムが実行されてしまう(※1)ことに問題がある。

(※1) CLASSID で指定された ActiveX コントロールがインストールされていない場合に、そのダウンロード先を指定するパラメータ。

(※2) CODEBASE パラメータに、リモートホスト上にあるプログラムへのパスを指定した場合、プログラムを実行するには、ターゲットの IE のセキュリティ設定で、“未署名の ActiveX コントロールのダウンロード” が有効に設定されている必要がある。しかし、この設定は IE のセキュリティ設定において、規定のレベルを“低”に設定しても有効とはならず、レベルのカスタマイズから“有効”を選択する必要がある。

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 NT 4.0 Server SP6a(J)	Internet Explorer	5.5	○
		5.5 SP1	○
		5.5 SP2	○
		6.0	○

検証結果

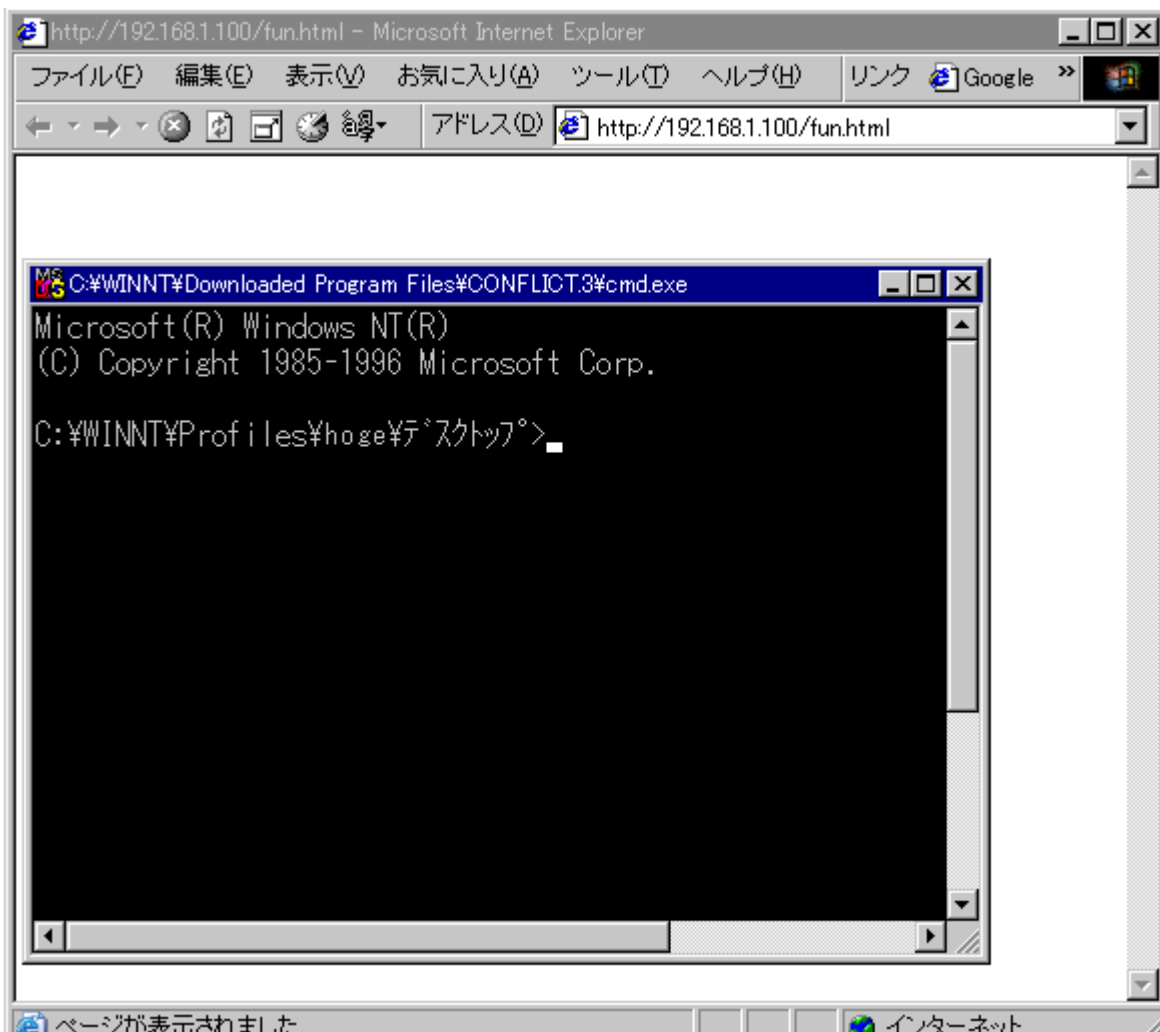
1) 検証環境

	OS	アプリケーション	備考
攻撃側	Windows NT 4.0 Server SP6a(J)	IIS 4.0	
ターゲット	Windows NT 4.0 Server SP6a(J)	Internet Explorer 5.5 SP2	
		Internet Explorer 6.0	

2) 検証結果

<CODEBASE パラメータに、ターゲットホスト上のプログラムを指定した場合>

IE 5.5 SP2 及び IE 6.0 において、下図のように、ターゲット側ホストで自動的にコマンドプロンプトが起動することが確認できた。



<CODEBASE パラメータに、リモートホスト上のプログラムを指定した場合>

コマンドプロンプトは起動しなかった。

そこで、IE のセキュリティ設定 → レベルのカスタマイズ → 未署名の ActiveX コントロールのダウンロード を“有効”に設定したところ、上記と同様の結果となった。

痕跡

1) ログ

ターゲットホストのイベントログには何も出力されなかった。

2) 痕跡

IE の履歴に参照した URL が残る他、Temporary Internet Files ディレクトリに参照した HTML ファイルが残る。

影響

悪意ある Web サイトの閲覧、もしくは電子メールの閲覧を行うことにより、攻撃者に任意のプログラムを実行されてしまう可能性がある。

影響を受けるOS、サービス

影響 ○:脆弱性あり、×:脆弱性なし

(2002/1/14現在)

OS	アプリケーション	バージョン	影響	備考
Windows 全般	Internet Explorer	6.0	○	

OS Windows 全般
アプリケーション Internet Explorer 6.0

対策方法

1) 対策

2002年1月24日現在、ベンダーからパッチなどはリリースされていない。暫定的な対策としては、下記が有効である。

- Internet Explorer のセキュリティ設定で、アクティブスクリプトを無効に設定する。

2) Advisory情報