

# Microsoft Windows Shell Remote Code Execution Vulnerability

分類 Design Error/受動的攻撃  
再現性 リモート/ローカル

## 技術解説

### 1)概要

Microsoft Windows には、Windows シェルを介して、実行可能でないオブジェクトからスクリプトコードが実行される問題がある。この問題が悪用された受動的攻撃により、ターゲット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 MS05-016 として公開されているものである。

## 対策方法

### 1)対策

Windows Server 2003, Windows XP, Windows 2000 は、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 (893086) 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。

Windows Millennium Edition, 98 は、2005年4月28日現在修正プログラムは提供されていない。参考サイトなどを参考にして対策を行う。

Windows Update :

<http://windowsupdate.microsoft.com/>

参考サイト:

<http://www.microsoft.com/japan/technet/security/bulletin/MS05-016.msp>

Microsoft HTML Application Host (以下「MSHTA」という。) を悪用した攻撃は、アプリケーションとの関連付けを無効にすることで回避可能である。

MSHTA を無効にする方法:

1. [スタート] をクリックして [ファイル名を指定して実行] を選択。
2. “%windir%\system32\mshta.exe /unregister” と入力し [OK] を押す。

### 2)Advisory情報

Microsoft Security Bulletin MS05-016 (英語版):

<http://www.microsoft.com/technet/security/bulletin/ms05-016.msp>

Microsoft Security Bulletin MS05-016 (日本語版):

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-016.msp>

SecurityFocus BID 13132:

<http://www.securityfocus.com/bid/13132>

iDEFENSE Security Advisory:

<http://www.idefense.com/application/poi/display?>

## 検証有無

結果 ○:成功、×:失敗、-:未検証

OS	ビルド	結果
Windows 2000 Advanced Server SP4 (J)	2195	○
Windows XP Professional SP1 (J)	2600.xpsp2.030422-1633	○
上記以外の組み合わせ		-

## 検証結果

### 1) 検証環境

OS	ビルド	備考
Windows 2000 Advanced Server SP4 (J)	5.00.2195	
Windows XP Professional SP1 (J)	2600.xpsp2.030422-1633	

## 痕跡

### 1) ログ

ターゲットホストのイベントログに、ログは出力されなかった。

### 2) 痕跡

攻撃に使用したファイルが残る。