

IE Remote URLMON.DLL Buffer Overflow Vulnerability

分類 Buffer Overflow/ 受動的攻撃
 関連ツール名称 urlmon-bo.pl
 再現性 リモート

技術解説

1) 概要

Internet Explorer (以降 IE と表記) 上で HTTP 通信を行う際に利用される URLMON.DLL に問題があり、大量の文字列が設定された HTTP 応答を受け取った場合に、バッファオーバーフローが発生する可能性がある。この問題により、攻撃者は、ログインしているユーザの権限で任意のコードを実行する可能性がある。

なお、この問題は Microsoft Security Bulletin MS03-015 として公開された 4 つの問題の内の 1 つとなる。

2) 原因

IE 上で HTTP 通信を行う際に利用される URLMON.DLL が、ある特定の HTTP 応答を受け取った際に、文字列長のチェックを適切に行わないことが原因である。

影響

ログインしているユーザの権限で、任意のコードを実行される可能性がある。

影響を受けるOS、サービス

影響 ○: 脆弱性あり、×: 脆弱性なし

(2003/7/2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	5.01	○	
		5.01 SP1	○	
		5.01 SP2	○	
		5.01 SP3	○	
		5.5	○	
		5.5 SP1	○	
		5.5 SP2	○	
		6.0	○	

		6.0 SP1	○	
--	--	---------	---	--

参考 URL:

<http://www.securityfocus.com/bid/7419>

対策方法

1)対策

この問題が対策済みである、MS03-015 (Q813489) の修正プログラムを適用する。

ダウンロード先:

<http://www.microsoft.com/windows/ie/downloads/critical/813489/default.asp>

2) Advisory情報

Microsoft Security Bulletin MS03-015(英語版):

<http://www.microsoft.com/technet/security/bulletin/MS03-015.asp>

Microsoft Security Bulletin MS03-015(日本語版):

<http://www.microsoft.com/japan/technet/security/bulletin/MS03-015.asp>

SecurityFocus BID 7419 :

<http://www.securityfocus.com/bid/7419>

Securiteam:

<http://www.securiteam.com/windowsntfocus/5NP050UAKY.html>

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 SP3 (J)	Internet Explorer	6.0 SP1 (Q813489 未適用)	○
上記以外の組み合わせ			-

検証結果

1)検証環境

	OS	アプリケーション	備考
攻撃側	Redhat Linux 7.1 (E)	Apache/1.3.27 (Unix)	
ターゲット	Windows 2000 Advanced Server SP3 (J)	Internet Explorer 6.0 SP1 (Q813489 未適用)	

2)検証結果

test.html を閲覧することで、IE が異常終了することを確認できた。

また、任意のコマンド実行が可能であると思われる。

痕跡

1) ログ

イベントログ(アプリケーション)に以下のエラーが出力される。

```
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: 2003/07/04
時刻: 14:28:56
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, unknown, 0.0.0.0, 41414141.
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 75 6e 6b 6e 6f in unkno
0038: 77 6e 20 30 2e 30 2e 30 wn 0.0.0
0040: 2e 30 20 61 74 20 6f 66 .0 at of
0048: 66 73 65 74 20 34 31 34 fset 414
0050: 31 34 31 34 31 0d 0a 14141..
```

2) 痕跡

IE のキャッシュフォルダ (C:¥Documents and Settings¥Administrator¥Local Settings¥Temporary Internet Files¥) に、test.html ファイルのみが残った。