

Multiple Vendor Telnet Client Remote Information Disclosure Vulnerability

分類 Access Validation Error/受動的攻撃
再現性 リモート

技術解説

1)概要

多くの製品に同梱されている telnet クライアントには、リモートから情報を搾取される問題がある。リモートの攻撃者は、Web ページや電子メールを介し IFRAME タグと "TELNET://" 形式の URL などを参照させ、telnet サーバに接続させることで、telnet クライアントのユーザ名またはアカウント名などの環境変数を搾取することが可能である。

マイクロソフト社はこの問題を、Microsoft Security Bulletin MS05-033 として公開している。

対策方法

1)対策

Windows を使用している場合は、Windows Update を利用することにより、マイクロソフト社より提供されている修正プログラム (896428) 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 以外は、各ベンダーから配布されているパッチを適用する。

【Microsoft Windows】

Windows Update :

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

参考サイト:

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-033.msp>

[Microsoft Windows Services for UNIX 3.5]

ダウンロードセンター:

<http://www.microsoft.com/downloads/details.aspx?familyid=7c3dd615-b82d-4520-9c3a-376283b01d5b&displaylang=en>

[Sun Microsystems]

Sun Update Connection - パッチとアップデート

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage>

2) Advisory情報

Microsoft Security Bulletin MS05-033 (英語版):

<http://www.microsoft.com/technet/security/bulletin/ms05-033.msp>

Microsoft Security Bulletin MS05-033 (日本語版):

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-033.msp>

Sun Alert ID: 101665:

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101665-1>

Sun Alert ID: 101671:

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101671-1>

iDEFENSE Security Advisory 06.14.05:

<http://idefense.com/application/poi/display?id=260&type=vulnerabilities&flashstatus=true>

SecurityFocus BID 13940:

<http://www.securityfocus.com/bid/13940>

検証有無

結果 ○:成功、×:失敗、-:未検証

OS	サービス	バージョン	結果
Windows XP Professional SP1 (J)	telnet	5.1.2600.1106	×
Solaris 8.0 sparc	telnet	-	○
上記以外の組み合わせ			-

検証結果

1) 検証環境

	OS	サービス	備考
攻撃側	Red Hat Linux 9 (E)	apache 1.3.33	netcat, perl が 必要
ターゲット	Windows XP Professional SP1 (J)	telnet 5.1.2600.1106	
	Solaris 8.0 sparc	telnet	

痕跡

1) ログ

<Windows XP Professional SP1 (J)>

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

ソース(S) : Application Error 分類(R) : なし 種類(E) : エラー イベントID(I) : 1000 エラー発生アプリケーション telnet.exe、バージョン 5.1.2600.1106、 エラー発生モジュール telnet.exe、バージョン 5.1.2600.1106、 エラー発生アドレス 0x00004b4b 詳細な情報は、 http://go.microsoft.com/fwlink/events.asp の [ヘルプとサポート センター] を参照してください。
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 74 65 6c ure tel 0018: 6e 65 74 2e 65 78 65 20 net.exe 0020: 35 2e 31 2e 32 36 30 30 5.1.2600 0028: 2e 31 31 30 36 20 69 6e .1106 in

```
0030: 20 74 65 6c 6e 65 74 2e telnet.  
0038: 65 78 65 20 35 2e 31 2e exe 5.1.  
0040: 32 36 30 30 2e 31 31 30 2600.110  
0048: 36 20 61 74 20 6f 66 66 6 at off  
0050: 73 65 74 20 30 30 30 30 set 0000  
0058: 34 62 34 62 0d 0a 4b4b..
```

<Solaris 8.0 sparc>

なし

2) 痕跡

<Windows XP Professional SP1 (J)>

IE の履歴に参照した URL が残るほか、Temporary Internet Files フォルダに、参照した HTML ファイルが残った。

<Solaris 8.0 sparc>

なし