

# Outlook-Outlook Express Malformed E-Mail Header

分類	Buffer Overflow
関連ツール名称	
再現性	リモート/ローカル

## 技術解説

### 1) 概要

メールヘッダーに改竄されたデータを大量に含ませることにより、OutlookもしくはOutlook Expressがバッファオーバーフローする問題がある。これにより、リモートユーザが電子メールクライアントのシステム上で任意のプログラムを実行出来てしまう可能性もある。

これは、電子メールクライアントが添付ファイルを開いたり、プログラムを実行することなく自動的に、トロイの木馬の実行、ワームの流布、標的となるホストのユーザレベルアクセスの奪取、ハードディスクのフォーマットといった無数の攻撃に使われる可能性を秘めている。

この問題が深刻な点はメールを受け取っただけで攻撃が成立してしまう点である。クライアントからサーバーのメールを削除出来ない為、サーバー管理者にメールを削除してもらわない限り、アプリケーションを起動し、メールをダウンロードする度にクラッシュを引き起こす。

### 2) 原因

この問題は、Outlook ExpressもしくはOutlookが、[POP3]もしくは[IMAP4]からメールをダウンロードした時に、メールの[Date:]行のGMT(※1)部を調べる方法に原因がある。この処理は、[INETCOMM.DLL]によって取り扱われる。これは、GMTによって表されるtokenを適切でない境界チェックをしているために生じる。従って、悪意を持ったユーザが、GMTの時刻値に異常に長い値を含んで特別に組み立てられた電子メールを送った場合には、バッファオーバーフローを発生させその結果、任意のプログラムを実行出来る可能性がある。

OutlookでMAPIサービス(※2)だけを使用するよう設定している場合は、この脆弱性の影響を受けない可能性もある。

※1: イギリスのグリニッジ天文台での天体観測を元に決められる時刻。昔は世界標準時刻として普及していたが、現在では原子時計によって決定されるUTC(協定世界時)が使われている。両者はほとんど同じだが、海の潮汐運動がブレーキとなり、地球の自転周期は年々長くなっているため、時間の経過と共にずれが生じる。UTCはGMTとのずれが0.8秒を超えると、「閏秒」を追加して差を詰める。

※2: メールソフト以外のアプリケーションから電子メールの機能を利用するためにマイクロソフトが提唱しているメールソフトの規格。MAPIに対応したメールソフトなら、ほかのアプリケーションソフトのメニューから直接メールを送信したり、モバイル機器で書いたメールをパソコンから送信したりなど、さまざまなソフト/ハードと連携して使うことができる。アウトLOOKやネットスケープメッセンジャーがMAPIに対応している。

# Outlook-Outlook Express Malformed E-Mail Header

## 検証有無

結果 ○:成功、×:失敗、-:未検証

(※1)バッファオーバーフローでアプリケーション強制終了

OS	アプリケーション	バージョン	結果
Windows	Outlook Express	4.0	-
		4.01	-
		5.0	○(※1)
		5.01	-
		5.5	×
	Outlook	97	-
		98	-
		2000	○(※)
上記以外			-

※Outlook Express 5がインストールされている場合、バッファオーバーフローでアプリケーション強制終了。

Outlook Express 5.5がインストールされている場合、メール受信OK。

## 検証結果

### 1) 検証環境

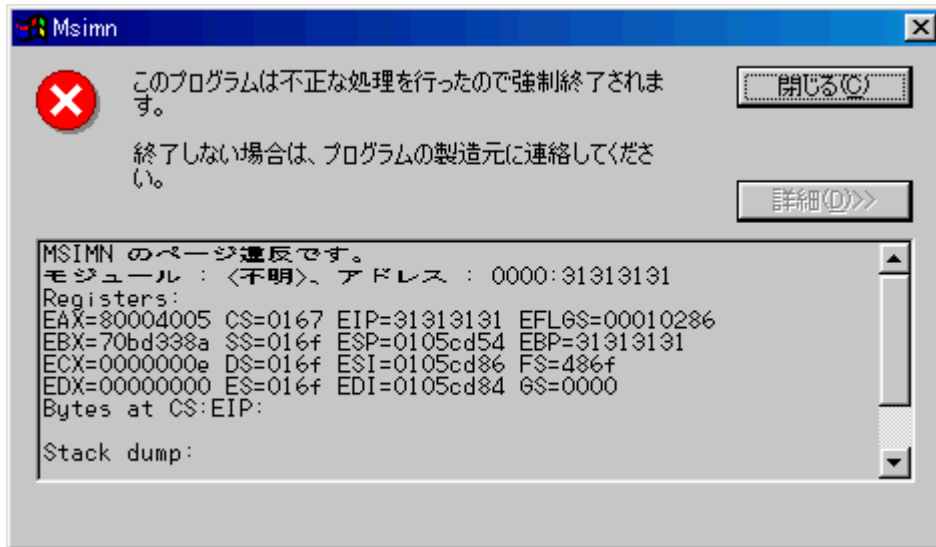
	OS	アプリケーション	備考
攻撃側	RedHat Linux 6.0J	-	
ターゲット	Windows 98 Second Edition	Internet Explorer Ver 5.00.2614.3500	検証パターン1
		Outlook Express 5 Ver 5.00.2314.1300	
		Outlook 2000	
	Windows NT Workstation 4.0	Internet Explorer 5 Ver 5.00.2614.3500	検証パターン2
		Outlook Express 5 Ver 5.00.2314.1300	
	Windows NT Sever 4.0	Internet Explorer 5.01 SP1 Ver 5.00.3105.0106	検証パターン3
Outlook Express 5.5 Ver 5.50.4133.2400			
Outlook 2000			

### 2) 検証結果

#### <検証パターン1>

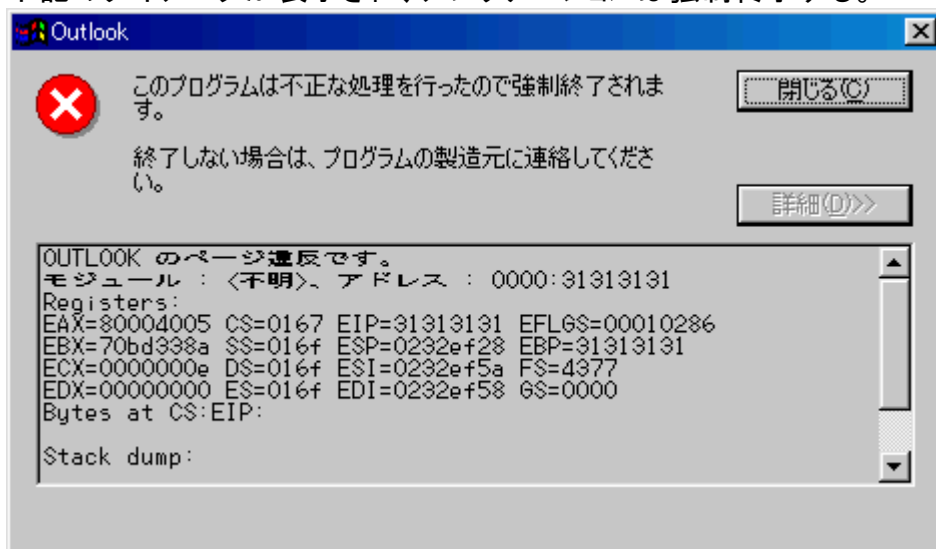
[Outlook Express 5の場合]

下記のダイアログが表示され、アプリケーションは強制終了する。



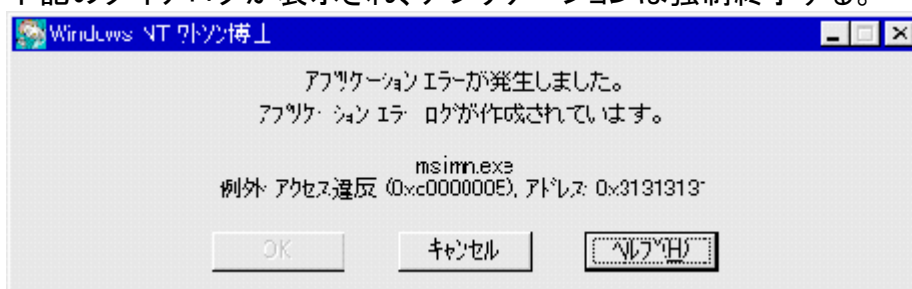
[Outlook Express 2000の場合]

下記のダイアログが表示され、アプリケーションは強制終了する。



<検証パターン2>

下記のダイアログが表示され、アプリケーションは強制終了する。



<検証パターン3>

[Outlook Express 5の場合]

正常にメールを受信

[Outlook Express 2000の場合]

メールの受信をしない

## 痕跡

### 1) ログ

なし

### 2) 痕跡

なし

## 影響

メールにヘッダーに改竄されたデータを含むことによりメールを受信しただけで、バッファオーバーフローさせる問題がある。その結果、トロイの木馬の実行、ワームの流布、標的となるホストのユーザレベルアクセスの奪取、ハードディスクのフォーマットといった無数の攻撃に使われる可能性がある。

## 影響を受けるOS、サービス

影響 ○:脆弱性あり、×:脆弱性なし

(2001/5/21現在)

OS	アプリケーション	バージョン	影響	備考
Windows	Microsoft Outlook Express	4.0	○	
		4.01	○	
		5.0	○	
		5.01	○	
	Microsoft Outlook	98	○	
		2000	○	
		97	×	

### ※影響をけるDLL

[ Inetcomm.dll ]

### インストールされているディレクトリ

Windows 98 C:¥Windows¥system

Windows NT C:¥Winnt¥system32

Vulnerability Version : 5.00.2314.1300

Fix Version : 5.50.4133.2400

(Outlook Expressのバージョンと同じ)

OS、サービス Microsoft Windows 95 / 98 / NT / 2000

アプリケーション Microsoft Outlook 98 / 2000、Microsoft Outlook Express 4.0 / 4.01 / 5.0 / 5.01

## 対策方法

### 1)対策

Internet Explorer 5.01 Service Pack 1かInternet Explorer 5.5をインストールする際に、Outlook Expressを5.5にアップグレードすることで、脆弱性を排除出来る。但しWindows2000がマシンにインストールされている場合は、Internet Explorer 5.5 をインストールしてもOutlook Expressはアップグレードしないので、脆弱性は排除出来ない。Windows 2000 Service Pack 1をインストールすることで、Internet Explorer 5.01 SP1とOutlook Express 5.5にアップグレードされ、脆弱性を排除出来る。

最新バージョン入手先 URL:  
[ 日本語版 ]

Internet Explorer 5.01 Service Pack 1  
[http://www.microsoft.com/windows/ie\\_intl/ja/download/ie501SP1.htm](http://www.microsoft.com/windows/ie_intl/ja/download/ie501SP1.htm)

Internet Explorer 5.5  
[http://www.asia.microsoft.com/windows/ie\\_intl/ja/download/ie55.htm](http://www.asia.microsoft.com/windows/ie_intl/ja/download/ie55.htm)  
(Windows 2000 以外の全てのプラットフォーム)

Windows 2000 Service Pack 1  
[http://www.microsoft.com/japan/windows2000/downloads/recommended/sp1/jpn\\_x86.asp](http://www.microsoft.com/japan/windows2000/downloads/recommended/sp1/jpn_x86.asp)  
(Windows 2000)

[ 英語版 ]

この脆弱性に対するパッチ  
<http://www.microsoft.com/windows/ie/download/critical/patch9.htm>

Internet Explorer 5.01 Service Pack 1  
<http://www.microsoft.com/Windows/ie/download/ie501sp1.htm>

Internet Explorer 5.5  
<http://www.microsoft.com/windows/ie/download/ie55.htm>  
(Windows 2000 以外の全てのプラットフォーム)

Windows 2000 Service Pack 1  
<http://www.microsoft.com/windows2000/downloads/recommended/sp1/x86DLType.asp>  
(Windows 2000)

Update情報  
<http://officeupdate.microsoft.com/2000/articles/oiMalformedHeader.htm>

### 2) Advisory情報

Microsoft

**英語版**

<http://www.microsoft.com/technet/security/bulletin/MS00-043.asp>

<http://www.microsoft.com/technet/security/bulletin/fq00-043.asp>

<http://www.microsoft.com/technet/support/kb.asp?ID=267884>

<http://officeupdate.microsoft.com/2000/articles/olMalformedHeader.htm>

**日本語版**

[http://www.microsoft.com/japan/technet/security/prekb.asp?sec\\_cd=MS00-043](http://www.microsoft.com/japan/technet/security/prekb.asp?sec_cd=MS00-043)

[http://www.microsoft.com/japan/technet/security/SecFaq.asp?sec\\_cd=ms00-043](http://www.microsoft.com/japan/technet/security/SecFaq.asp?sec_cd=ms00-043)

<http://www.microsoft.com/JAPAN/support/kb/articles/JP267/8/84.htm>

**CIAC**

<http://ciac.llnl.gov/ciac/bulletins/k-060.shtml>

**X-Force**

<http://xforce.iss.net/alerts/advise57.php>

**NIPC**

<http://www.nipc.gov/warnings/advisories/2000/00-050.htm>

**Windows IT Security**

<http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=9539>