

アタックテストサービス エクスプレスご利用のお客様へ

2007年1月11日  
富士通株式会社

マイクロソフト製品における脆弱性について

拝啓、貴社益々ご清栄の事とお喜び申し上げます。  
平素は格別なるご高配を賜りまして、厚く御礼申し上げます。

この度、「マイクロソフト製品における脆弱性」に関する情報が1月10日に Qualys 社より報告されました。

これらの脆弱性をご利用の対象機器に検出されないことを、下記の【確認方法】に従って、アタックテストサービスエクスプレスでご確認ください。

敬具

記

Qualys アラートアドバイザリ(英文)

Microsoft Security Bulletin: Multiple Security Vulnerabilities  
<http://www.qualys.com/research/alerts/view.php/2007-01-09>

【MS07-001】

『Microsoft Office 2003 のポルトガル語（ブラジル）の文章校正プログラムの脆弱性により、リモートでコードが実行される』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-001.msp>  
<http://www.microsoft.com/japan/security/bulletins/ms07-001e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-001.msp>

#### 【MS07-002】

『Microsoft Excel の脆弱性により、リモートでコードが実行される』

#### [関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-002.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-002e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-002.msp>

#### 【MS07-003】

『Microsoft Outlook の脆弱性により、リモートでコードが実行される』

#### [関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-003.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-003e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms07-003.msp>

#### 【MS07-004】

『Vector Markup Language の脆弱性により、リモートでコードが実行される』

#### [関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-004.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-004e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-004.msp>

#### 【確認方法】

##### ■特定の脆弱性を指定した、ホストの診断

以下の方法にて、本脆弱性のみを選択して短時間で診断することが可能です。

- 1) QualysGuard にログインし、“Preferences”->“Options”->“Profiles”より“New Profile”を作成します。
- 2) “Scanned TCP Ports”オプションの“None”を選択し、“Additional”にチェックを入れ、TCP ポート「135,139」を記入します。
- 3) “Vulnerability Detection”オプションの「Custom」を選択し、“Configure...”をクリックします。  
Find を「QID」、within を「All」、containing で以下の QualysID を指定して“Search”し、以下の QualysID を選択して“OK”を押してください。

Qualys ID: 110051

『Microsoft Office 2003 のポルトガル語（ブラジル）の文書校正プログラムの脆弱性により、リモートでコードが実行される（MS07-001）（Microsoft Office 2003 Brazilian Portuguese Grammar Checker Remote Code Executi[...]）』

Qualys ID: 110050

『Microsoft Excel に、リモートでコードを実行される脆弱性（MS07-002）（Microsoft Excel Remote Code Execution Vulnerabilities (MS07-002)）』

Qualys ID: 110049

『Microsoft Outlook に、リモートでコードが実行される脆弱性（MS07-003）（Microsoft Outlook Remote Code Execution Vulnerabilities (MS07-003)）』

Qualys ID: 90377

『Vector Markup Language の脆弱性により、リモートでコードが実行される（MS07-004）（Microsoft Windows Vector Markup Language Remote Code Execution Vulnerability (MS07-004)）』

※もし、Windows(NetBIOS)マシン名でホストの脆弱性を調査したい場合には QualysID:82044 『ホスト名の発見』も選択し、そして UDP ポート「137」のスキャンも可能としてください。

- 4) “Windows Authentication”オプションの“Enable Windows authentication”をチェックします。
- 5) “Profile Title”をつけ、最後に“Save”します。
- 6) “Scan”->“Launch Scan”で診断対象の IP を選択し、作成した

“Options” を選択し、“Start Scan”します。

---

お問い合わせ窓口)

富士通株式会社 セキュリティサービス統括部 基盤サービス部

qualys-support@support.fujitsu.com

<http://segroup.fujitsu.com/secure/service/attacktest-express/index.html>