

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2月15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2月15日に Qualys 社より報告されました。

これらの脆弱性が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ー(英文)

Microsoft Security Bulletin: February 2007 Security Bulletin

<http://www.qualys.com/research/alerts/view.php/2007-02-13>

【MS07-005】

『ステップ バイ ステップの対話型トレーニングの脆弱性により、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/MS07-005.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-005e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-005.msp>

【MS07-006】

『Windows シェルの脆弱性により、特権が昇格される』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-006.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-006e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-006.msp>

【MS07-007】

『Windows Image Acquisition サービス の脆弱性により、特権が昇格される』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-007.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-007e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-007.msp>

【MS07-008】

『HTML ヘルプの ActiveX コントロールの脆弱性により、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/MS07-008.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-008e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-008.msp>

【MS07-009】

『Microsoft Data Access Components 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/MS07-009.msp>x

<http://www.microsoft.com/japan/security/bulletins/ms07-009e.msp>x

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-009.msp>x

【MS07-010】

『Microsoft Malware Protection Engine 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/MS07-010.msp>x

<http://www.microsoft.com/japan/security/bulletins/ms07-010e.msp>x

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-010.msp>x

【MS07-011】

『Microsoft OLE ダイアログの脆弱性により、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/MS07-011.msp>x

<http://www.microsoft.com/japan/security/bulletins/ms07-011e.msp>x

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-011.msp>x

【MS07-012】

『Microsoft MFC 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/MS07-012.msp>x

<http://www.microsoft.com/japan/security/bulletins/ms07-012e.msp>x

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-012.msp>x

【MS07-013】

『Microsoft リッチ エディットの脆弱性により、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/MS07-013.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-013e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-013.msp>

【MS07-014】

『Microsoft Word 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/MS07-014.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-014e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-014.msp>

【MS07-015】

『Microsoft Office 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/MS07-015.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-015e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-015.msp>

【MS07-016】

『Internet Explorer 用の累積的なセキュリティ更新プログラム』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-016.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-016e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-016.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: 90379

ステップバイステップの対話型トレーニングに、リモートのコード実行を許可する脆弱性 (MS07-005) (Step-by-Step Interactive Training Could Allow Remote Code Execution (MS07-005))

Qualys ID: 90380

Windows シェルに、特権昇格を許可する脆弱性 (MS07-006) (Windows Shell Could Allow Privilege Elevation (MS07-006))

Qualys ID: 90384

Windows Image Acquisition サービスに、特権昇格を許可する脆弱性 (MS07-007) (Windows Image Acquisition Service Could Allow Privilege Elevation (MS07-007))

Qualys ID: 90383

HTML ヘルプの ActiveX コントロールに、リモートのコード実行を許可する脆弱性 (MS07-008) (HTML Help ActiveX Control Could Allow Remote Code Execution (MS07-008))

Qualys ID: 90385

Microsoft Data Access Components (MDAC) に、リモートのコード実行を許可する脆弱性 (MS07-009) (Microsoft Data Access Components Could Allow Remote Code Execution (MS07-009))

Qualys ID: 90382

Microsoft Malware Protection Engine に、リモートのコード実行を許可する脆弱性 (MS07-010) (Microsoft Malware Protection Engine Could Allow Remote Code Execution (MS07-010))

Qualys ID: 90378

Microsoft OLE ダイアログに、リモートのコード実行を許可する脆弱性 (MS07-011) (Microsoft OLE Dialog Could Allow Remote Code Execution (MS07-011))

Qualys ID: 90381

Microsoft MFC に、リモートのコード実行を許可する脆弱性 (MS06-012) (Microsoft MFC Could Allow Remote Code Execution (MS07-012))

Qualys ID: 110054

Microsoft リッチエディットに、リモートのコード実行を許可する脆弱性 (MS07-013) (Microsoft RichEdit Could Allow Remote Code Execution (MS07-013))

Qualys ID: 110052

Microsoft Word 2000 の脆弱性により、リモートでコードが実行される - ゼロデイ (Microsoft Word 2000 Vulnerability Could Allow Remote Code Execution - Zero Day)

Qualys ID: 110053

Microsoft Office に、リモートでコードが実行される脆弱性 - ゼロデイ (Microsoft Office Could Allow Remote Code Execution - Zero Day)

Qualys ID: 100045

Internet Explorer の累積的なセキュリティ更新 (MS07-016)

(Cumulative Security Update for Internet Explorer (MS07-016))

※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>