

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

2006年6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6月13日
付けで Qualys 社より報告されました。

これらのセキュリティ情報の対象となる脆弱性が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: June 2006 Security Bulletin
<http://www.qualys.com/research/alerts/view.php/2006-06-13>

【MS06-021】

『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/MS06-021.msp>

<http://www.microsoft.com/japan/security/bulletins/MS06-021e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS06-021.msp>

【MS06-022】

『ART の画像表示の脆弱性により、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/MS06-022.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-022e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-022.msp>

【MS06-023】

『Microsoft JScript 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/MS06-023.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-023e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-023.msp>

【MS06-024】

『Windows Media Player 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/MS06-024.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-024e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-024.msp>

【MS06-025】

『ルーティングとリモート アクセスの脆弱性により、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/MS06-025.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-025e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-025.msp>

【MS06-027】

『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/MS06-027.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-027e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-027.msp>

【MS06-028】

『Microsoft PowerPoint 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/MS06-028.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-028e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-028.msp>

【MS06-029】

『Outlook Web Access を実行する Microsoft Exchange Server の脆弱性により、スクリプト インジェクションが起こる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-029.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-029e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-029.msp>

【MS06-030】

『サーバー メッセージ ブロックの脆弱性により、特権が昇格される』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-030.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-030e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-030.msp>

【MS06-031】

『RPC の相互認証の脆弱性により、なりすましが行なわれる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-031.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-031e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-031.msp>

【MS06-032】

『TCP/IP 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/MS06-032.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-032e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-032.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”してください。

◆和訳データにつきましては鋭意準備中です。

Qualys ID: 100035

『Internet Explorer の累積的なパッチの未適用 (MS06-021)
(Cumulative Security Update for Internet Explorer Missing
(MS06-021)) 』

Qualys ID: 90317

『Microsoft に ART 画像の表示により、リモートでコードが実行される脆弱性 (MS06-022) (Microsoft ART Image Rendering Remote Code Execution Vulnerability (MS06-022)) 』

Qualys ID: 90320

『Microsoft JScript にリモートでコードを実行される脆弱性 (MS06-023) (Microsoft JScript Remote Code Execution Vulnerability (MS06-023)) 』

Qualys ID: 90314

『Microsoft Windows Media Player の PNG 画像処理に脆弱性 (MS06-024) (Microsoft Windows Media Player PNG Vulnerability (MS06-024)) 』

Qualys ID: 90319

『Windows のルーティングとリモートアクセスに、リモートからコードを実行される脆弱性 (MS06-025) (Windows Routing and Remote Access Could Allow Remote Code Execution

(MS06-025)) 』

Qualys ID: 90312

『Microsoft Word の脆弱性により、リモートのコード実行が許可される(MS06-027) (Vulnerability in Microsoft Word Could Allow Remote Code Execution (MS06-027)) 』

Qualys ID: 90315

『Microsoft PowerPoint の脆弱性により、リモートのコード実行が許可される(MS06-028) (Vulnerability in Microsoft PowerPoint Could Allow Remote Code Execution (MS06-028)) 』

Qualys ID: 90318

『Outlook Web Access を動作する Microsoft Exchange Server の脆弱性により、スクリプトインジェクションが許可される(MS06-029) (Vulnerability in Microsoft Exchange Server Running Outlook Web Access Could Allow Script Inje[...]) 』

Qualys ID: 90323

『Microsoft Windows の SMB に特権昇格の脆弱性(MS06-030) (Microsoft Windows SMB Could Allow Elevation of Privileges (MS06-030)) 』

Qualys ID: 90322

『Microsoft RPC に相互認証のなりすましの脆弱性(MS06-031) (Microsoft RPC Mutual Authentication Spoofing Vulnerability (MS06-031)) 』

Qualys ID: 90316

『TCP / IP の脆弱性により、リモートのコード実行が許可される(MS06-032) (Vulnerability in TCP/IP Could Allow Remote Code Execution (MS06-032)) 』

※もし、Windows(NetBIOS)マシン名でホストの脆弱性を調査したい時には 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、先程作成した “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>