

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8月9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8月9日
付けで 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: August 2006 Security Bulletin
<http://www.qualys.com/research/alerts/view.php/2006-08-08>

【MS06-040】

『Server サービスの脆弱性により、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/ms06-040.mspx>

<http://www.microsoft.com/japan/security/bulletins/ms06-040e.mspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx>

【MS06-041】

『DNS 解決の脆弱性により、リモートでコードが実行される』

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-041.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-041e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-041.msp>

【MS06-042】

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

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-042.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-042e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-042.msp>

【MS06-043】

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

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-043.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-043e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-043.msp>

【MS06-044】

『Microsoft 管理コンソール (MMC) の脆弱性により、リモートでコードが実行される』

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-044.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-044e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-044.msp>

【MS06-045】

『Windows エクスプローラ の脆弱性により、リモートでコードが実行される』

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-045.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-045e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-045.msp>

【MS06-046】

『HTML ヘルプの脆弱性により、リモートでコードが実行される』

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-046.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-046e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-046.msp>

【MS06-047】

『Microsoft Visual Basic for Applications (VBA) の脆弱性により、
リモートでコードが実行される』

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-047.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-047e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-047.msp>

【MS06-048】

『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]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-048.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-048e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-048.msp>

【MS06-049】

『Windows カーネルの脆弱性により、特権が昇格される』

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-049.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-049e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-049.msp>

【MS06-050】

『Microsoft Windows ハイパーリンク オブジェクト ライブラリの脆弱性により、リモートでコードが実行される』

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-050.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-050e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-050.msp>

【MS06-051】

『Windows カーネルの脆弱性により、リモートでコードが実行される』

[関連 URL]

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-051.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-051e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-051.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: 90336

『Vulnerability in Server Service Could Allow Remote Code Execution (MS06-040)』

Qualys ID: 90337

『Vulnerability in DNS Resolution Could Allow Remote Code Execution (MS06-041) 』

Qualys ID: 100036

『Microsoft Cumulative Security Update for Internet Explorer (MS06-042)』

Qualys ID: 90340

『Microsoft Windows Remote Code Execution Vulnerability (MS06-043)』

Qualys ID: 90345

『Microsoft Management Console Remote Code Execution Vulnerability (MS06-044) 』

Qualys ID: 90344

『Microsoft Windows Explorer Remote Code Execution Vulnerability (MS06-045) 』

Qualys ID: 90343

『Microsoft HTML Help Remote Code Execution Vulnerability

(MS06-046)』

Qualys ID: 90341

『Microsoft Visual Basic for Applications Remote Code Execution Vulnerability (MS06-047) 』

Qualys ID: 110038

『Microsoft PowerPoint Remote Code Execution Vulnerabilities (MS06-048) 』

Qualys ID: 90339

『Microsoft Windows Kernel Privilege Elevation Vulnerability (MS06-049)』

Qualys ID: 90338

『Microsoft Windows Hyperlink Object Library Remote Code Execution Vulnerabilities (MS06-050) 』

Qualys ID: 90342

『Microsoft Windows Kernel Remote Code Execution Vulnerability (MS06-051) 』

※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、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>