

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7月12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7月11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: July 2006 Security Bulletin
<http://www.qualys.com/research/alerts/view.php/2006-07-11>

【MS06-033】

『ASP.NET の脆弱性により、情報漏えいが起こる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-033.msp>

<http://www.microsoft.com/japan/security/bulletins/MS06-033e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS06-033.msp>

【MS06-034】

『Active Server Pages を使用した Internet Information Services (IIS) 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/MS06-034.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-034e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-034.msp>

【MS06-035】

『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/MS06-035.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-035e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-035.msp>

【MS06-036】

『DHCP クライアント 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/MS06-036.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-036e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-036.msp>

【MS06-037】

『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/MS06-037.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-037e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-037.msp>

【MS06-038】

『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/MS06-038.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-038e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-038.msp>

【MS06-039】

『Microsoft Office フィルタの脆弱性により、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/MS06-039.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-039e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-039.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: 90330

『ASP.NET Could Allow Information Disclosure (MS06-033)』

Qualys ID: 90328

『Microsoft Internet Information Services Remote Code
Execution Vulnerability (MS06-034) 』

Qualys ID: 90329

『Microsoft Windows Server Driver Remote Code Execution
Vulnerability (MS06-035) 』

Qualys ID: 90327

『Microsoft Windows DHCP Client Service Remote Code
Execution Vulnerability (MS06-036) 』

Qualys ID: 110034

『Excel の脆弱性により、リモートコードの実行が許可される
- ゼロデイ (Vulnerability in Excel Could Allow Remote
Code Execution - Zero Day) 』

Qualys ID: 110035

『Vulnerabilities in Microsoft Office Could Allow Remote
Code Execution (MS06-038) 』

Qualys ID: 110036

『Vulnerabilities in Microsoft Office Filters Could Allow
Remote Code Execution (MS06-039) 』

※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>