

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

平成 17 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複数の脆弱性について

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複数の脆弱性」に関する情報が 6 月 14 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 セキュリティアドバイザリ（英文）

Microsoft Security Bulletin: Multiple Security Vulnerabilities
<http://www.qualys.com/research/alerts/view.php/2005-06-14>

【MS05-025】

『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/ms05-025.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-025e.msp>

（英文）

<http://www.microsoft.com/technet/security/bulletin/MS05-025.msp>

【MS05-026】

『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]

（日本文）

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-026.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-026e.msp>

（英文）

<http://www.microsoft.com/technet/security/bulletin/MS05-026.aspx>

【MS05-027】

『サーバー メッセージ ブロックの脆弱性により、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/ms05-027.aspx>

<http://www.microsoft.com/japan/security/bulletins/ms05-027e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-027.aspx>

【MS05-028】

『WebClient 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/ms05-028.aspx>

<http://www.microsoft.com/japan/security/bulletins/ms05-028e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-028.aspx>

【MS05-029】

『Exchange Server 5.5 の Outlook Web Access の脆弱性により、クロスサイト スクリプティング攻撃が行われる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-029.aspx>

<http://www.microsoft.com/japan/security/bulletins/ms05-029e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-029.aspx>

【MS05-030】

『Outlook Express 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/ms05-030.aspx>

<http://www.microsoft.com/japan/security/bulletins/ms05-030e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-030.aspx>

【MS05-031】

『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/ms05-031.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-031e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-031.msp>

【MS05-032】

『Microsoft エージェントの脆弱性により、なりすましが行われる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-032.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-032e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-032.msp>

【MS05-033】

『Telnet クライアントの脆弱性により、情報漏えいが起こる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-033.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-033e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-033.msp>

【MS05-034】

『ISA Server 2000 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/ms05-034.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-034e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-034.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: 90252

『Microsoft SMB Remote Code Execution Vulnerability (MS05-027)』

Qualys ID: 90253

『Microsoft HTML Help Remote Code Execution Vulnerability (MS05-026)』

Qualys ID: 90254

『Microsoft Outlook Web Access for Exchange Server Cross-Site Scripting Vulnerability (MS05-029)』

Qualys ID: 90255

『Microsoft ISA Server 2000 Cumulative Update Missing (MS05-034)』

Qualys ID: 90256

『Microsoft Windows Web Client Service Remote Code Execution Vulnerability (MS05-028)』

Qualys ID: 90257

『Microsoft Step-by-Step Interactive Training Could Allow Remote Code Execution (MS05-031)』

Qualys ID: 90258

『Outlook Express News Reading Vulnerability (MS05-030)』

Qualys ID: 90259

『Microsoft Agent Content-Spoofing Vulnerability (MS05-032)』

Qualys ID: 90260

『Vulnerability in Microsoft Windows Telnet Client Could Allow Information Disclosure (MS05-033)』

Qualys ID: 100026

『Cumulative Security Update For Internet Explorer Missing (MS05-025)』

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。

Risk Matrix Report による、影響のあるホストの予測

以下の方法にて、実際に診断をする前に上記の脆弱性がお客様のホストに影響があるかどうかを推測することが可能です。

- 1) "Preferences"->"Setup"で、"Business Risk"を設定します。
Business Risk は、ホストのクリティカル性と、検出された脆弱性の重大性をもとに計算されます。
- 2) "Preferences"->"Asset Group"で、対象とするホストを選択し、「Edit」をクリック、「Business Info」にて"Business Impact"を選択します。
- 3) "Report"->"Scan Reports"の、"Risk Matrix Report"の「Run」アイコンをクリックします。
- 4) Risk Matrix Report の画面で、上記の「Qualys ID」を選択し、"Select Report Target"で診断したい Asset Group もしくは IP アドレスを選択、「Run」をクリックします。
- 5) Risk Matrix Report が生成され、対処すべきホストが優先順位の高い順に表示されます。

- 以上 -

お問い合わせ窓口)

富士通株式会社 アウトソーシング事業本部

セキュリティサービス統括部 IT マネージセンター

qualys-support@support.fujitsu.com

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