

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2月10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
2月8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/2005-02-08>

【MS05-004】

『ASP.NET パス検証の脆弱性』

[関連URL]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-004.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-004e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-004.msp>

【MS05-005】

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

[関連URL]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-005.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-005e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-005.msp>

【MS05-006】

『Windows SharePoint Services および SharePoint Team Services の脆弱性
により、クロスサイト スクリプティングおよびなりすましの攻撃が行われる』

[関連URL]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-006.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-006e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-006.msp>

【MS05-007】

『Windows の脆弱性により、情報漏えいが起こる』

[関連URL]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-007.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-007e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-007.msp>

【MS05-008】

『Windows シェルの脆弱性により、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/ms05-008.msp>
<http://www.microsoft.com/japan/security/bulletins/ms05-008e.msp>
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS05-008.msp>

【MS05-009】
『PNG 処理の脆弱性により、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/ms05-009.msp>
<http://www.microsoft.com/japan/security/bulletins/ms05-009e.msp>
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS05-009.msp>

【MS05-010】
『ライセンス ログ サービスの脆弱性により、コードが実行される』

[関連URL]
(日本文)
<http://www.microsoft.com/japan/technet/security/bulletin/ms05-010.msp>
<http://www.microsoft.com/japan/security/bulletins/ms05-010e.msp>
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS05-010.msp>

【MS05-011】
『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/ms05-011.msp>
<http://www.microsoft.com/japan/security/bulletins/ms05-011e.msp>
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS05-011.msp>

【MS05-012】
『OLE および COM 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/ms05-012.msp>
<http://www.microsoft.com/japan/security/bulletins/ms05-012e.msp>
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS05-012.msp>

【MS05-013】
『DHTML 編集コンポーネントの Active X 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/ms05-013.msp>
<http://www.microsoft.com/japan/security/bulletins/ms05-013e.msp>
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS05-013.msp>

【MS05-014】
『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/ms05-014.msp>
<http://www.microsoft.com/japan/security/bulletins/ms05-014e.msp>
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS05-014.msp>

【MS05-015】

『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]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-015.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-015e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-015.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: 90220

『Microsoft ASP.NET Path Validation Vulnerability (MS05-004)』

Qualys ID: 90221

『Microsoft Windows License Logging Service Could Allow Code Execution (MS05-010)』

Qualys ID: 90222

『Microsoft Windows SharePoint Services Could Allow Cross-Site Scripting and Spoofing Attacks (MS05-006)』

Qualys ID: 90223

『Microsoft Windows Shell Remote Code Execution (MS05-008)』

Qualys ID: 90224

『Microsoft Windows Remote Information Disclosure (MS05-007)』

Qualys ID: 90225

『Vulnerability in Microsoft Office XP Could Allow Remote Code Execution (MS05-005)』

Qualys ID: 90227

『Windows Media Player and Messenger Remote Code Execution (MS05-009)』

Qualys ID: 90228

『Microsoft Windows OLE and COM Remote Code Execution (MS05-012)』

Qualys ID: 90229

『DHTML Editing Component ActiveX Control Remote Code Execution (MS05-013)』

Qualys ID: 90230

『Microsoft Server Message Block Remote Code Execution (MS05-011)』

Qualys ID: 90231

『Microsoft Hyperlink Object Library Buffer Overflow (MS05-015)』

Qualys ID: 100024

『Microsoft Internet Explorer Cumulative Update (MS05-014)』

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>