

平成17年10月12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
10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 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/2005-10-11>

【MS05-044】

『Windows FTP クライアントの脆弱性により、ファイルの転送場所が改ざんされる』

[関連URL]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-044.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-044e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-044.msp>

【MS05-045】

『ネットワーク接続マネージャの脆弱性により、サービス拒否が起こる』

[関連URL]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-045.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-045e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-045.msp>

【MS05-046】

『NetWare 用クライアント 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]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-046.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-046e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-046.msp>

【MS05-047】

『プラグ アンド プレイの脆弱性により、リモートでコードが実行され、ローカルで特権の昇格が行なわれる』

[関連URL]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/ms05-047.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-047e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-047.msp>

【MS05-048】

『Microsoft Collaboration Data Objects 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/ms05-048.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-048e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-048.msp>

【MS05-049】

『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/ms05-049.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-049e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-049.msp>

【MS05-050】

『DirectShow 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/ms05-050.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-050e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-050.msp>

【MS05-051】

『MSDTC 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/ms05-051.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-051e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-051.msp>

【MS05-052】

『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/ms05-052.msp>

<http://www.microsoft.com/japan/security/bulletins/ms05-052e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS05-052.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「135,139,445」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: 90277

『Microsoft Windows FTP Client Transfer Location Tampering Vulnerability (MS05-044)』

Qualys ID: 90281

『Microsoft Network Connection Manager Denial of Service Vulnerability (MS05-045)』

Qualys ID: 90280

『Microsoft Windows Client Service For Netware Buffer Overflow Vulnerability (MS05-046)』

ity (MS05-046)』

Qualys ID: 90278

『Microsoft Plug and Play Remote Code Execution and Local Privilege Elevation Vulnerability (MS05-047)』

Qualys ID: 90275

『Microsoft Collaboration Data Objects Remote Code Execution (MS05-048)

』

Qualys ID: 90273

『Microsoft Windows Shell Remote Code Execution Vulnerability (MS05-049)

』

Qualys ID: 90276

『Microsoft DirectShow Remote Code Execution Vulnerability (MS05-050)』

Qualys ID: 90274

『Microsoft MSDTC and COM+ Remote Code Execution Vulnerability (MS05-051)

)』

Qualys ID: 100030

『Microsoft Internet Explorer Cumulative Patch Missing (MS05-052)』

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>