

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 16 年 10 月 14 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(2004 年 10 月)

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 12 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 Critical Microsoft Security Vulnerabilities

<http://www.qualys.com/research/alerts/view.php/2004-10-12>

【MS04-029】

『RPC ランタイム ライブラリの脆弱性により、情報漏えいおよびサービス
拒否が起こる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/ms04-029.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-029e.asp

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS04-029.msp>

【MS04-030】

『WebDav XML Message ハンドラの脆弱性によりサービス拒否が起こる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/ms04-030.asp>
http://www.microsoft.com/japan/security/security_bulletins/MS04-030e.asp
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS04-030.mspx>

【MS04-031】

『 NetDDE 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/ms04-031.asp>
http://www.microsoft.com/japan/security/security_bulletins/MS04-031e.asp
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS04-031.mspx>

【MS04-032】

『 Microsoft Windows の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/ms04-032.asp>
http://www.microsoft.com/japan/security/security_bulletins/MS04-032e.asp
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS04-032.mspx>

【MS04-033】

『 Microsoft Excel 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/ms04-033.asp>
http://www.microsoft.com/japan/security/security_bulletins/MS04-033e.asp
(英文)
<http://www.microsoft.com/technet/security/bulletin/MS04-033.mspx>

【MS04-034】

『 圧縮 (zip 形式) フォルダの脆弱性により、コードが実行される 』

[関連 URL]

(日本文)
<http://www.microsoft.com/japan/technet/security/bulletin/ms04-034.asp>
http://www.microsoft.com/japan/security/security_bulletins/MS04-034e.asp

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS04-034.mspx>

【MS04-035】

『SMTP 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/ms04-035.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-035e.asp

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx>

【MS04-036】

『NNTP 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/ms04-036.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-036e.asp

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS04-036.mspx>

【MS04-037】

『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/ms04-037.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-037e.asp

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx>

【MS04-038】

『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/ms04-038.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-038e.asp

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS04-038.mspx>

【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。

Qualys ID: 90190

『Microsoft RPC におけるランタイムライブラリのサービス不能 (DoS) (MS04-029)』

Qualys ID: 90188

『WebDAV における XML メッセージハンドラのサービス不能 (DoS) (MS04-030)』

Qualys ID: 90184

『NetDDE の脆弱性によるリモートからのコード実行 (MS04-031)』

Qualys ID: 90186

『Microsoft Windows における複数の脆弱性 (MS04-032)』

Qualys ID: 90187

『Microsoft Excel におけるリモートからのコード実行 (MS04-033)』

Qualys ID: 90183

『(zip 形式で) 圧縮されたフォルダにおけるリモートからのコード実行脆弱性 (MS04-034)』

Qualys ID: 74167

『Microsoft Exchange 2003 におけるリモートコード実行 (MS04-035)』

Qualys ID: 90185

『Microsoft NNTP におけるリモートからのコード実行脆弱性 (MS04-036)』

Qualys ID: 90189

『Windows シェルにおけるリモートからのコード実行 (MS04-037)』

Qualys ID: 100018

『Microsoft Internet Explorer における複数の脆弱性 (MS04-038)』

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 セキュリティシステム部

qualys-support@support.fujitsu.com

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