

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 12 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
12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ー（英文）

Microsoft Security Bulletin: Multiple Security Vulnerabilities

<http://www.qualys.com/research/alerts/view.php/2004-12-14>

【MS04-041】

『WordPad 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/ms04-041.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-041e.asp

（英文）

<http://www.microsoft.com/technet/security/bulletin/MS04-041.msp>

【MS04-042】

『DHCP の脆弱性により、リモートでコードが実行され、サービス拒否が起こる』

[関連 URL]

（日本文）

<http://www.microsoft.com/japan/technet/security/bulletin/ms04-042.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-042e.asp

（英文）

<http://www.microsoft.com/technet/security/bulletin/MS04-042.msp>

【MS04-043】

『ハイパー ターミナルの脆弱性により、コードが実行される』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/ms04-043.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-043e.asp

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS04-043.mspx>

【MS04-044】

『Windows カーネルおよび LSASS の脆弱性により、特権の昇格が起こる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/ms04-044.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-044e.asp

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS04-044.mspx>

【MS04-045】

『WINS 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/ms04-045.asp>

http://www.microsoft.com/japan/security/security_bulletins/MS04-045e.asp

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS04-045.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。

『 Microsoft WINS のバッファオーバーフローの脆弱性 (MS04-045) 』

Qualys ID: 90201

『 Microsoft Windows のローカル特権の昇格 (MS04-044) 』

Qualys ID: 90202

『 Microsoft WordPad のリモートからのコード実行 (MS04-041) 』

Qualys ID: 90203

『 Microsoft DHCP のリモートコード実行およびサービス拒否 (MS04-042) 』

Qualys ID: 115036

『 Microsoft ハイパー ターミナルのリモートコード実行 (MS04-043) 』

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 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>