

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

2006 年 12 月 14 日
富士通株式会社

マイクロソフト製品における脆弱性について

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脆弱性」に関する情報が 12 月 13 日に Qualys 社より報告されました。

これらの脆弱性をご利用の対象機器に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 アラートアドバイザリ(英文)

Microsoft Security Bulletin: Multiple Security Vulnerabilities
<http://www.qualys.com/research/alerts/view.php/2006-12-12>

【MS06-076】

『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/MS06-076.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-076e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-076.msp>

【MS06-072】

『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/MS06-072.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-072e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-072.msp>

【MS06-073】

『Visual Studio 2005 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/MS06-073.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-073e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-073.msp>

【MS06-078】

『Windows Media Format 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/MS06-078.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-078e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-078.msp>

【MS06-074】

『SNMP 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/MS06-074.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-074e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-074.mspix>

【MS06-077】

『リモート インストール サービス (RIS) 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/MS06-077.mspix>

<http://www.microsoft.com/japan/security/bulletins/ms06-077e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-077.mspix>

【MS06-075】

『Windows の脆弱性により、特権が昇格される』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-075.mspix>

<http://www.microsoft.com/japan/security/bulletins/ms06-075e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-075.mspix>

【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”を押し
てください。

Qualys ID: 90368

『Outlook Express の累積的なセキュリティ更新 (MS06-076)
(Cumulative Security Update for Outlook Express (MS06-076))』

Qualys ID: 90371

『Internet Explorer の累積的なセキュリティ更新 (MS06-072)
(Cumulative Security Update for Internet Explorer (MS06-072))』

Qualys ID: 115448

『Visual Studio 2005 の脆弱性により、リモートでコードが実行される (MS06-073)
(Visual Studio 2005 Vulnerability Could Allow Remote Code Execution (MS06-073))』

Qualys ID: 90367

『Windows Media Format の脆弱性により、リモートでコードを実行される (MS06-078)
(Windows Media Format Vulnerability Could Allow Remote Code Execution (MS06-078))』

Qualys ID: 90372

『SNMP にリモートでコードを実行される脆弱性 (MS06-074)
(SNMP Remote Code Execution Vulnerability (MS06-074))』

Qualys ID: 90370

『リモートインストールサービスにリモートでコードを実行される脆弱性 (MS06-077)
(Remote Installation Service Remote Code Execution Vulnerability (MS06-077))』

Qualys ID: 90369

『Windows の特権昇格の脆弱性 (MS06-075)
(Windows Privilege Elevation Vulnerability (MS06-075))』

※もし、Windows(NetBIOS)マシン名でホストの脆弱性を調査したい
場合には 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、作成した “Options” を選択し、“Start Scan”します。

お問い合わせ窓口)

富士通株式会社 セキュリティサービス統括部 基盤サービス部

qualys-support@support.fujitsu.com

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