

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

2007年9月12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、9月11日に Qualys 社より報告されました。

これらの脆弱性が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、ご確認ください。

敬具

記

Qualys アラートアドバイザー(英文)

Microsoft Security Bulletin: September 2007 Security Bulletin
<http://www.qualys.com/research/alerts/view.php/2007-09-11>

【MS07-051】

『Microsoft エージェントの脆弱性により、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/MS07-051.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-051e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-051.msp>

【MS07-052】

『Crystal Reports for Visual Studio 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/MS07-052.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-052e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-052.msp>

【MS07-053】

『Windows Services for UNIX 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/MS07-053.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-053e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-053.msp>

【MS07-054】

『MSN Messenger および Windows Live Messenger 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/MS07-054.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-054e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-054.msp>

【確認方法】

以下の方法にて、本脆弱性のみを選択した短時間な診断を実施することが可能です。

- 1) QualysGuard にログインします。
- 2) 画面左側の「メニュー・ペイン」より、「Option Profiles」

メニューをクリックします。

- 3) 画面上部の「メニュー・バー」より、「New: Option Profile」メニューをクリックします。
- 4) 「New Option Profile」ウインドウの右下に配置されている「Advanced」ボタンをクリックします。
- 5) 「TCP Ports」オプションの「None」ラジオボタンをクリックします。
- 6) 「Additional」チェックボックスにチェックを入れ、TCP ポート「135,139」を入力します。
- 7) 「Vulnerability Detection」オプションの「Custom」ラジオボタンをクリックし、「Configure...」ボタンをクリックします。
- 8) 「Configure...」ウインドウ画面上部の「メニュー・バー」より、「Serch」メニューをクリックし、以下の Qualys ID で検出後、「OK」をクリックします。

Qualys ID: 90408

Vulnerability in Microsoft Agent Could Allow Remote Code Execution (MS07-051)

Qualys ID: 90409

Vulnerability in Crystal Reports for Visual Studio Could Allow Remote Code Execution (MS07-052)

Qualys ID: 115630

Windows Services for UNIX Could Allow Elevation of Privilege (MS07-053)

Qualys ID: 115620

MSN Messenger Video Conversation Buffer Overflow Vulnerability (MS07-054)

◆和訳データにつきましては鋭意準備中です。

※診断結果に、Windows(NetBIOS)マシン名を表示させたい場合には、Qualys ID:82044 『ホスト名の発見』を選択し、UDP ポート「137」を指定してください。

- 9) 「Authentication」オプションの「Enable Windows authentication」チェックボックスをチェックします。
- 10) 「Option Profile Title」をつけ、最後に「Save」をクリックします。
- 11) 画面左側の「メニュー・ペイン」より、「Scan」メニューをクリック

します。

- 12) 画面上部の「メニュー・バー」より、「New: Scan」メニューをクリックします。
- 13) 「Launch Scan」ウインドウ画面の「Target Hosts」にて診断対象の IP をクリックします。
- 14) 「Options」にて作成した「Options Profile:」をクリックします。
- 15) 「Launch」ボタンをクリックします。

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>