

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8月16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、8月14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: August 2007 Security Bulletin

<http://www.qualys.com/research/alerts/view.php/2007-08-14>

【MS07-042】

『XML コア 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]

(日本文)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS07-042.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-042e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-042.msp>

【MS07-043】

『OLE オートメーションの脆弱性により、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/MS07-043.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-043e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-043.msp>

【MS07-044】

『Microsoft Excel 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/MS07-044.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-044e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-044.msp>

【MS07-045】

『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/MS07-045.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-045e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-045.msp>

【MS07-046】

『GDI 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/MS07-046.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-046e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-046.mspx>

【MS07-047】

『Windows Media Player 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/MS07-047.mspx>

<http://www.microsoft.com/japan/security/bulletins/ms07-047e.mspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms07-047.mspx>

【MS07-048】

『Windows ガジェットの脆弱性により、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/MS07-048.mspx>

<http://www.microsoft.com/japan/security/bulletins/MS07-048e.mspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-048.mspx>

【MS07-049】

『Virtual PC および Virtual Server 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/MS07-049.mspx>

<http://www.microsoft.com/japan/security/bulletins/MS07-049e.mspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-049.mspx>

【MS07-050】

『Vector Markup Language 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/MS07-050.msp>

<http://www.microsoft.com/japan/security/bulletins/MS07-050e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-050.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: 90405

Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS07-042)

Qualys ID: 90404

Vulnerability in OLE Automation could allow remote code execution (MS07-043)

Qualys ID: 110063

Microsoft Excel Could Allow Remote Code Execution (MS07-044)

Qualys ID: 100050

Cumulative Security Update for Internet Explorer (MS07-045)

Qualys ID: 90407

Vulnerability in GDI Could Allow Remote Code Execution (MS07-046)

Qualys ID: 90406

Vulnerabilities in Windows Media Player Could Allow Remote Code Execution (MS07-047)

Qualys ID: 115613

Windows Gadgets Could Allow Remote Code Execution (MS07-048)

Qualys ID: 115612

Virtual PC and Virtual Server Could Allow Elevation of Privilege (MS07-049)

Qualys ID: 100051

Vulnerability in Vector Markup Language Could Allow Remote Code Execution (MS07-050)

◆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>