

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4月11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、4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リ(英文)

Microsoft Security Bulletin: February 2007 Security Bulletin  
<http://www.qualys.com/research/alerts/view.php/2007-04-10>

【MS07-018】

『Microsoft Content Management Server 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/MS07-018.msp>  
<http://www.microsoft.com/japan/security/bulletins/ms07-018e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-018.msp>

**【MS07-019】**

『ユニバーサル プラグ アンド プレイの脆弱性により、リモートでコードが実行される』

[関連 URL]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-019.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-019e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-019.msp>

**【MS07-020】**

『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]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-020.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-020e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-020.msp>

**【MS07-021】**

『CSRSS の脆弱性により、リモートでコードが実行される』

[関連 URL]

(日本語)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-021.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-021e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/MS07-021.msp>

## 【MS07-022】

『Windows カーネルの脆弱性により、特権が昇格される』

### [関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/bulletin/MS07-022.msp>

<http://www.microsoft.com/japan/security/bulletins/ms07-022e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms07-022.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: 12236

Microsoft Content Management Server Could Allow Remote Code Execution  
(MS07-018)

Qualys ID: 90390

Universal Plug and Play Could Allow Remote Code Execution  
(MS07-019)

Qualys ID: 90392

Vulnerability in Microsoft Agent Could Allow Remote Code Execution  
(MS07-020)

Qualys ID: 90374 90376

Microsoft Windows に CSRSS の情報開示の脆弱性 - ゼロデイ  
(Microsoft Windows CSRSS Information Disclosure Vulnerability - Zero Day)  
(MS07-021)

Qualys ID: 90391

Microsoft Windows に CSRSS の情報開示の脆弱性 - ゼロデイ  
(Microsoft Windows CSRSS Information Disclosure Vulnerability - Zero Day)  
(MS07-022)

※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>