

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10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10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、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ー(英文)

Microsoft Security Bulletin: Multiple Security Vulnerabilities

<http://www.qualys.com/research/alerts/view.php/2006-10-10>

【MS06-056】

『ASP.NET 2.0 の脆弱性により、情報漏えいが起こる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-056.mspx>

<http://www.microsoft.com/japan/security/bulletins/ms06-056e.mspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-056.mspx>

【MS06-057】

『Windows Explorer 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/MS06-057.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-057e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-057.msp>

**【MS06-058】**

『Microsoft PowerPoint 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/MS06-058.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-058e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-058.msp>

**【MS06-059】**

『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/MS06-059.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-059e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-059.msp>

**【MS06-060】**

『Microsoft Word 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/MS06-060.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-060e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-060.aspx>

**【MS06-061】**

『Microsoft 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/MS06-061.aspx>

<http://www.microsoft.com/japan/security/bulletins/ms06-061e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-061.aspx>

**【MS06-062】**

『Microsoft Office 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/MS06-062.aspx>

<http://www.microsoft.com/japan/security/bulletins/ms06-062e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-062.aspx>

**【MS06-063】**

『Server サービスの脆弱性により、サービス拒否が起こる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-063.aspx>

<http://www.microsoft.com/japan/security/bulletins/ms06-063e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-063.aspx>

**【MS06-064】**

『TCP/IP IPv6 の脆弱性により、サービス拒否が起こる』

[関連 URL]

(日本文)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-064.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-064e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-064.msp>

【MS06-065】

『Windows オブジェクト パッケージの脆弱性により、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/MS06-065.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-065e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-065.msp>

【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: 90357

『Microsoft ASP.NET 2.0 に情報開示の脆弱性 (MS06-056)  
(Microsoft ASP.NET 2.0 Information Disclosure Vulnerability  
(MS06-056)) 』

Qualys ID: 90352

『Microsoft Windows Explorer にリモートでコードを実行される脆弱  
性 (MS06-057) (Microsoft Windows Explorer Remote Code  
Execution Vulnerability (MS06-057)) 』

Qualys ID: 110043

『Microsoft PowerPoint にリモートでコードを実行される複数の脆弱  
性 (MS06-058) (Microsoft PowerPoint Multiple Remote Code  
Execution Vulnerabilities (MS06-058)) 』

Qualys ID: 110045

『Microsoft Excel にリモートでコードを実行される複数の脆弱性  
(MS06-059) (Microsoft Excel Multiple Remote Code Execution  
Vulnerabilities (MS06-059)) 』

Qualys ID: 110046

『Microsoft Word にリモートでコードを実行される脆弱性  
(MS06-060) (Microsoft Word Remote Code Execution  
Vulnerabilities (MS06-060)) 』

Qualys ID: 90356

『Microsoft XML コアサービスにリモートでコードを実行される脆弱  
性 (MS06-061) (Microsoft XML Core Services Remote Code  
Execution Vulnerability (MS06-061)) 』

Qualys ID: 110044

『Microsoft Office にリモートでコードを実行される脆弱性  
(MS06-062) (Microsoft Office Remote Code Execution  
Vulnerabilities (MS06-062)) 』

Qualys ID: 90354

『Microsoft Server サービスにサービス不能(DoS)の脆弱性  
(MS06-063) (Microsoft Server Service Denial of  
Service Vulnerability (MS06-063)) 』

Qualys ID: 90353

『Microsoft の TCP/IP IPv6 にサービス不能(DoS)の脆弱性  
(MS06-064) (Microsoft TCP/IP IPv6 Denial of Service  
Vulnerabilities (MS06-064)) 』

Qualys ID: 90355

『Microsoft Windows のオブジェクトパッケージャにリモートでコー  
ドを実行される脆弱性(MS06-065) (Microsoft Windows Object  
Packager Remote Code Execution Vulnerability (MS06-065)) 』

※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>