

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 11 月 15 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 11 月 15 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ー(英文)

Microsoft Security Bulletin: Multiple Security Vulnerabilities

<http://www.qualys.com/research/alerts/view.php/2006-11-14>

【MS06-066】

『NetWare 用クライアント 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/MS06-066.aspx>

<http://www.microsoft.com/japan/security/bulletins/ms06-066e.aspx>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-066.aspx>

**【MS06-067】**

『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/MS06-067.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-067e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-067.msp>

**【MS06-068】**

『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/MS06-068.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-068e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-068.msp>

**【MS06-069】**

『Adobe の Macromedia Flash 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/MS06-069.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-069e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-069.msp>

**【MS06-070】**

『Workstation 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]

(日本語)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-070.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-070e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-070.msp>

【MS06-071】

『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]

(日本語)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS06-071.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-071e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-071.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: 90363

『NetWare 用クライアントサービスに、リモートでコードを実行される複数の脆弱性 (MS06-066) (Client Service for NetWare Multiple Remote Code Execution Vulnerabilities (MS06-066))』

Qualys ID: 100038

『Internet Explorer 用の累積的なセキュリティ更新プログラム (MS06-067) (Cumulative Security Update for Internet Explorer (MS06-067))』

Qualys ID: 90364

『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 (MS06-068) (Microsoft Agent Vulnerability Could Allow Remote Code Execution (MS06-068))』

Qualys ID: 115409

『Adobe Flash Player にリモートからコードを実行される複数の脆弱性 (APSB06-11) (MS06-069) (Adobe Flash Player Multiple Remote Code Execution Vulnerabilities (APSB06-11) (MS06-069))』

Qualys ID: 90365

『Workstation 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 (MS06-070) (Vulnerability in Workstation Service Could Allow Remote Code Execution (MS06-070))』

Qualys ID: 90361

『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 (MS06-071) (Microsoft XML Core Services Remote Code Execution Vulnerability (MS06-071))』

※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>