

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9月28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28日に Qualys 社より報告されました。

これらの脆弱性に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: Microsoft VML Security Vulnerabilities
<http://www.qualys.com/research/alerts/view.php/2006-09-27>

【MS06-055】

『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/MS06-055.msp>

<http://www.microsoft.com/japan/security/bulletins/ms06-055e.msp>

(英文)

<http://www.microsoft.com/technet/security/bulletin/ms06-055.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”してください。

Qualys ID: 100039

『Vector Markup Language Remote Code Execution Vulnerability
- IE Unpatched (MS06-055)』

Qualys ID: 90351

『Vulnerability in Vector Markup Language Could Allow Remote
Code Execution (MS06-055) 』

※もし、Windows(NetBIOS)マシン名でホストの脆弱性を調査したい時には 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。

※現在、診断結果に出力される脆弱性につきましては、英語となっております。日本語データにつきましては鋭意準備中です。

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>