

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

平成 16 年 8 月 12 日
富士通株式会社

「Exchange Server 5.5 Outlook Web Access の脆弱性」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、「Exchange Server 5.5 Outlook Web Access の脆弱性」に関する情報が
8 月 10 日付けで Qualys 社より報告されました。

下記の方法に従って、アタックテストサービスエクスプレスで本脆弱性が検出
されないかをご確認ください。万が一検出された場合には、至急対処のご検討を
していただきますようお願いいたします。

敬具

記

Qualys セキュリティアドバイザリ（英文）

Microsoft Security Bulletin: Moderate Exchange 5.5 OWA Vulnerability (MS04-026)
<http://www.qualys.com/research/alerts/view.php/2004-08-10>

【MS04-026】

Exchange Server 5.5 Outlook Web Access の脆弱性により、クロスサイト ス
クリプティングと詐称による攻撃が実行される

[関連 URL]

（日本文）

http://www.microsoft.com/japan/security/security_bulletins/MS04-026e.asp
<http://www.microsoft.com/japan/technet/security/bulletin/MS04-026.asp>

（英文）

<http://www.microsoft.com/technet/security/bulletin/ms04-026.msp>

[確認方法]

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「135,139,445」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」, 以下の Qualys ID で containing を "Search"し、その QualysID を選択して"OK"してください。

Qualys ID: 90162

「Microsoft Exchange Server 5.5 Outlook Web Access XSS and Spoofing Vulnerability (MS04-026)」

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、先程作成した"Options"を選択し、"Start Scan"します。

- 以上 -

お問い合わせ窓口)

富士通株式会社 アウトソーシング事業本部

セキュリティサービス統括部 セキュリティシステム部

qualys-support@support.fujitsu.com

<http://segroup.fujitsu.com/secure/service/attacktest-express/index.html>