

平成 16 年 4 月 15 日  
富士通株式会社

マイクロソフト社 Windows、RPC/DCOM、Outlook Express、  
JET データベースエンジンの脆弱性について

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、マイクロソフト社 Windows、RPC/DCOM、Outlook Express、JET データベースエンジンの脆弱性が 4 月 14 日付けで Qualys 社より報告されました。

下記の方法に従って、QualysGuard 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

【Windows の脆弱性】

QualysID 90108 :

「Microsoft Windows における複数の脆弱性  
(Multiple Microsoft Windows Vulnerabilities (MS04-011))」

[脆弱性の詳細について]

Microsoft Windows に複数の脆弱性が報告されています。詳細は以下のマイクロソフト社の情報をご参照してください。

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS04-011.asp>

[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「25,80,135,139,443,445,593」を記入します。
- 3) "Scan Dead Hosts"オプションの"Include dead hosts in scans"をチェックします。
- 4) "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 を「90108」として"Search"し、QualysID「90108」を選択

して"OK"してください。

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「82004」も選択してください。

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。

#### 【RPC/DCOM の脆弱性】

QualysID 68528 :

「Microsoft Windows RPC/DCOM における複数の脆弱性  
(Multiple Microsoft Windows RPC/DCOM Vulnerabilities (MS04-012))」

[脆弱性の詳細について]

Microsoft Windows の RPC/DCOM サービスに脆弱性が報告されています。詳細は以下のマイクロソフト社の情報をご参照してください。

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS04-012.asp>

[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「25,80,135,139,443,445,593」を記入します。

3) "Scan Dead Hosts"オプションの"Include dead hosts in scans"をチェックします。

4) "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 を「68528」として"Search"し、QualysID「68528」を選択して"OK"してください。

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「82004」も選択してください。

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。

#### 【Outlook Express の脆弱性】

QualysID 90110 :

「Microsoft Outlook Express の累積セキュリティアップデートがインストールされていない  
(Microsoft Outlook Express Cumulative Security Update Not Installed (MS04-013))」

[脆弱性の詳細について]

Microsoft Outlook Express に脆弱性が報告されています。詳細は以下のマイクロソフト社の情報をご参照してください。

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS04-013.asp>

[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"->"Option"->"Authentication"より"New Record"を作成します。
- 2) "Domain Information"オプションで、ドメインレベルにて認証を行なう場合には「Domain」を、ローカルホストレベルでの任書すを行なう場合は「Local」を選択し、Windows ドメイン名を入力します。
- 3) 「Windows User Name:」に、認証に使用されるユーザアカウントを、「Windows Password:」、「Confirm Password:」に対応するパスワードを入力します。
- 4) "IP s"で、認証のために全てのホストを選択してください。
- 5) Save ボタンをクリックし、設定を保存します。
- 6) 次に、"Preferences"->"Options"->"Profiles"より"New Profile" を作成します。
- 7) "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「139,445」を記入します。
- 8) "Scan Dead Hosts"オプションの"Include dead hosts in scans"をチェックします。
- 9) "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 を「90110」として"Search"し、QualysID「90110」を選択して"OK"してください。

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「82004」も選択してください。

- 10) "Windows Authentication"オプションの"Enable Windows authentication"をチェックします。
- 11) "Profile Title"をつけ、最後に"Save"します。
- 12) "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。

---

【Jet データベースエンジンの脆弱性】

QualysID 19089 :

「Microsoft Jet データベースエンジンのバッファオーバーフローの脆弱性  
(Microsoft Jet Database Engine Buffer Overflow Vulnerability (MS04-014))」

[脆弱性の詳細について]

Microsoft Jet データベースエンジンの脆弱性が報告されています。詳細は以下のマイクロソフト社の情報をご参照してください。

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS04-014.asp>

[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"->"Option"->"Authentication"より"New Record"を作成します。
  - 2) "Domain Information"オプションで、ドメインレベルにて認証を行なう場合には「Domain」を、ローカルホストレベルでの任書すを行なう場合は「Local」を選択し、Windows ドメイン名を入力します。
  - 3) 「Windows User Name:」に、認証に使用されるユーザアカウントを、「Windows Password:」、「Confirm Password:」に対応するパスワードを入力します。
  - 4) "IP s"で、認証のために全てのホストを選択してください。
  - 5) Save ボタンをクリックし、設定を保存します。
  - 6) 次に、"Preferences"->"Options"->"Profiles"より"New Profile" を作成します。
  - 7) "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「139,445」を記入します。
  - 8) "Scan Dead Hosts"オプションの"Include dead hosts in scans"をチェックします。
  - 9) "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 を「19089」として"Search"し、QualysID「19089」を選択して"OK"してください。
- 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「82004」も選択してください。
- 10) "Windows Authentication"オプションの"Enable Windows authentication"をチェックします。
  - 11) "Profile Title"をつけ、最後に"Save"します。
  - 12) "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>

担当：長谷川、安立、松本