

平成 16 年 3 月 11 日
富士通株式会社

マイクロソフト社 Windows Media サービス、MSN Messenger、Outlook 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、マイクロソフト社の Windows Media サービス、MSN Messenger、Outlook の脆弱性が 3 月 9 日付けで Qualys 社より報告されました。

なお、Windows Media サービスの脆弱性は、Qualys 社にて独自に発見したものです。

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 Media サービスの脆弱性】

QualysID 90105 :

「Microsoft Windows Media サービスにおけるリモートのサービス不能 (DoS)脆弱性 (Microsoft Windows Media Services Remote Denial of Service Vulnerability)」

[影響を受けるソフトウェア]

Microsoft Windows 2000 Server Service Pack 2、Service Pack 3、および Service Pack 4

[脆弱性の詳細について]

攻撃者は、Windows 2000 Server で動作する Windows Media Station サービスまたは、Windows Media Monitor Service の でこの脆弱性を悪用し、特別な細工をした一連のパケットを WINS サーバーに送信し、サービスを異常終了させる可能性があります。これにより、サービス拒否が起こる可能性があります。機能を回復するためには、サービスを手動で再起動する必要があります。

[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) "Selective Vulnerability Scanning"オプションの「Performing selective vulnerability scanning」を選択し、"Config"を行ないます。
- Find を「Qualys ID」、within を「All」、containing を「90105」として "Search"し、QualysID 「90105」

を選択して"OK"してください。

3) "Scanned TCP Ports"オプションの、"Partial"->"Standard"のチェックをはずし、代わりに"Additional"で、TCP ポート「139,445,7007」を選択します。

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

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。

4) "Profile Title"をつけ、最後に"Save"します。

5) "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。

[関連文書]

Qualys セキュリティアラート (英文)

Multiple MSFT Vulnerabilities

<http://www.qualys.com/docs/securityalerts/Qadvise-Multiple-MSFT-20040309.pdf>

Microsoft セキュリティ情報 [MS04-008]

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/ms04-008.asp>

【Outlook の脆弱性】

QualysID 105010 :

「Microsoft Outlook の Mailto 解析における任意のプログラム実行の脆弱性 (Microsoft Outlook Mailto Arbitrary Code Execution Vulnerability)」

[影響を受けるソフトウェア]

Microsoft Office XP Service Pack 2

Microsoft Outlook 2002 Service Pack 2

[脆弱性の詳細について]

この脆弱性により攻撃者はインターネットエクスプローラを通してローカルのコンピュータ上でスクリプトコードを実行できます。

[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) "Vulnerability Detection"オプションの「Custom」を選択し、"Configure..." をクリックします。
Find を「Qualys ID」、within を「All」、containing を「105010」として "Search"し、QualysID「105010」を選択して"OK"してください。
- 8) "Scanned TCP Ports"オプションの、"None"を選択し、"Additional"に TCP ポート「139,445」を入力し、チェックを入れます。
"Scan Dead Hosts"オプションの"Include dead hosts in scans"をチェックします。
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。
- 9) "Windows Authentication"オプションの"Enable Windows authentication"をチェックします。
- 10) "Profile Title"をつけ、最後に"Save"します。
- 11) "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。

[関連文書]

Qualys セキュリティアラート (英文)

Multiple MSFT Vulnerabilities

<http://www.qualys.com/docs/securityalerts/Qadvise-Multiple-MSFT-20040309.pdf>

Microsoft セキュリティ情報 [MS04-009]

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/ms04-009.asp>

【MSN Messenger の脆弱性】

QualysID 90106 :

「MSN Messenger 6 が許可する情報開示 (MSN Messenger 6 Allows Information Disclosure)」

[影響を受けるソフトウェア]

Microsoft MSN Messenger 6.0

Microsoft MSN Messenger 6.1

[脆弱性の詳細について]

攻撃者は、MSN Messenger のユーザにこの脆弱性を悪用し、特別な細工をした一連のパケットを送信することによりハードディスク上のファイルを参照することができます。

[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) "Vulnerability Detection"オプションの「Custom」を選択し、"Configure..." をクリックします。

Find を「Qualys ID」、within を「All」、containing を「90106」として "Search"し、QualysID「90106」を選択して"OK"してください。

8) "Scanned TCP Ports"オプションの、"None"を選択し、"Additional"に TCP ポート「139,445」を入力し、チェックを入れます。

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

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。

9) "Windows Authentication"オプションの"Enable Windows authentication"をチェックします。

10) "Profile Title"をつけ、最後に"Save"します。

11) "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。

[関連文書]

Qualys セキュリティアラート (英文)

Multiple MSFT Vulnerabilities

<http://www.qualys.com/docs/securityalerts/Qadvise-Multiple-MSFT-20040309.pdf>

Microsoft セキュリティ情報 [MS04-010]

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/ms04-010.asp>

- 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

電話：044-754-3353