

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 15 年 8 月 25 日  
富士通株式会社

Qualys 社からの「Nachi Worm」に関するアラートメールについて

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。

8 月 21 日、8 月 23 日に、Qualys 社より送付されました、「Nachi Worm」に関するアラートメールにつきまして、ご報告いたします。

下記の方法に従って QualysGuard で本脆弱性を検出し、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

[差出人] Qualys <Qualys@Qualys.com>

[表題] Security Alert: Nachi Worm (8 月 21 日送付)  
Security Alert: Signature Update for Nachi Worm (8 月 23 日送付)

[主な内容]

7 月 16 日に発表されました、Windows RPC DCOM のセキュリティホール(CAN-2003-0352)に加え、3 月 17 日に発表されました、Windows 2000 のコンポーネントに存在した別のセキュリティホール(CAN-2003-0109)を悪用する、MSBlaster の亜種が脅威を振るっております。

以下の方法にて、本ワームの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。

[確認方法]

- 1) QualysGuard にログインし、"Preferences" -> "Options" で "New Option" を作成します。
- 2) "Selective Vulnerability Scanning" オプションの「Performing selective vulnerability scanning」を選択し、"Configure" を行ないます。QualysID 「1113」, 「68517」, 「86479」を選択して "OK" してください。
- 3) "Scanned TCP Ports" オプションの、"Partial" -> "Additional" で、「135-139, 445, 593」ポートのみを選択します。  
"Scan Dead Hosts" オプションの "Include dead hosts in scans" をチェックします。
- 4) "Options 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。

[ご参考]

Nachi Worm の検出 (Nachi Worm Detected)

Nachi Worm は「Microsoft Windows における DCOM RPC インタフェースのバッファオーバーラン脆弱性」(Qualys ID : 68518)、および、「Microsoft Windows 2000 における WebDAV のバッファオーバーフロー脆弱性」(Qualys ID : 86479)の脆弱性について攻撃をしかける Worm です。MSBlaster と違い PING(ICMP)も送信しますが、Smurf 攻撃の脅威はございません。また、このワームは、Network Associates では、「Nachi Worm」と命名されておりますが、別名「WORM\_MSBLAST.D」(トレンドマイクロ)、「Welchia Worm」(Symantec)、「Welchi」(F-secure)とも呼ばれております。

関連 URL

【Microsoft】

- ・MS03-026 : RPC インタフェースのバッファ オーバーランによりコードが実行される  
<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS03-026.asp>

【Cert】

- ・CVEID CAN-2003-0352  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352>
- ・CVEID CAN-2003-0109  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109>

- 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](mailto: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