

平成 15 年 8 月 14 日
富士通株式会社

「W32/MSBlaster」ワームの脆弱性について

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 RPC の脆弱性を攻略する新種ワームが、2003 年 8 月 12 日に発見されました。本脆弱性は、パソコン起動時にワームが実行されるように変更したり、ランダムに感染対象を検索し、感染拡大を計る恐れがあります。

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

【「W32/MSBlaster」ワームの脆弱性】

QualysID 68518 (CVE ID :CAN-2003-0352)

「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 (Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability)」

QualysID 90064

「msblast.exe」DCOM ワームの検出 (The 'msblast.exe' DCOM Worm Detected)」

[本脆弱性の対象]

Windows NT Server 4.0

Windows NT Server 4.0, Terminal Server Edition

Windows 2000

Windows XP

Windows Server 2003

[本脆弱性の影響]

TCP/IP でメッセージの送受信を処理する、RPC のある特定の箇所に脆弱性が存在します。攻撃者は不正な RPC メッセージを送信し、コンピュータの RPC サービスを異常終了させ、任意のコードを実行する可能性があります。

これにより、たとえば Web ページの変更、ハード ディスクの再フォーマット、新規のユーザーをローカル管理者グループに追加するなど、そのサーバー上で任意の操作を実行される恐れがあります。

このワームは、感染したシステムの日付が2003年8月16日になるとwindowsupdate.com に DoS 攻撃を開始します。さらに、再起動時にワームも再起動するように、自分自身をレジストリに追加します。また、脆弱なマシンを見つけると攻撃を開始し、感染拡大を試みます。

[確認方法]

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。

- 1) QualysGuard にログインし、"Preferences" -> "Options" で "New Option" を作成します。
- 2) "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。
- 3) 次に、"Selective Vulnerability Scanning" オプションの Performing selective vulnerability scanning」を選択し、"Config" を行ないます。
- 4) Find を Name、within を All、containing を DCOM」とし "Search" し、Qualys ID 68518 と90064 を選択して "OK" してください。
- 5) "Options 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。
- 7) QualysID 68518 が検出された場合、至急パッチをあててください。QualysID 90064 が検出された場合は、既にワームに感染している恐れがありますので、至急対策が必要となります。

イントラネット診断サービスをご利用のお客様へ

通常、インターネットに接続されているコンピュータでは該当のポートはファイアウォールでブロックされていますが、イントラネット環境ではアクセスすることが可能です。

イントラネット診断サービスをご契約のお客様は効果的にチェックすることが可能ですので、合わせてご利用いただきますようよろしくお願いいたします。

[対処]

Microsoft は、この問題に対してパッチを提供しています。

RPC インターフェイスのバッファ オーバーランによりコードが実行される(823980) (MS03-026) 」

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS03-026.asp>
を参照してください。

回避法として、ホスト上で DCOM を無効にすることができます。これは、ユーティリティ "dcomcnfg" を使用すると、実行することができます。Windows XP などでは、変更を有効にするために再起動が必要となります。

感染してしまった場合は、Windows ディレクトリに作成されたプログラムファイル (msblast.exe) の削除とレジストリの修正が必要となります。

[ご参考]

IPA セキュリティセンター

新種ワーム「W32/MSBlaster」に関する情報

<http://www.ipa.go.jp/security/topics/newvirus/msblaster.html>

- 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