

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 2 月 12 日
富士通株式会社

Windows インターネットネームサービス(WINS)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 インターネットネームサービス(WINS)を攻撃対象とし、リモートでコードを実行する脆弱性が、2 月 10 日付けで Qualys 社より報告されました。なお、この脆弱性は、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

【MS WINS の脆弱性】

QualysID 90104 :

「Microsoft WINS におけるバッファオーバーフロー脆弱性 (Microsoft WINS Buffer Overflow Vulnerability)」

[影響を受けるシステム]

Microsoft Windows NT Server 4.0
Microsoft Windows NT Server 4.0, TSE
Microsoft Windows 2000 Server
Microsoft Windows Server 2003

[脆弱性の詳細について]

Windows インターネットネームサービス(WINS)にセキュリティ上の脆弱性が存在します。この脆弱性は、特別に細工されたパケットの長さを WINS が検証する方法に問題があるために起こります。

攻撃者は、Windows Server 2003 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「90104」として"Search" し、QualysID 「90104」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。
- 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「42,139,445」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) "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)

Microsoft WINS Vulnerability

<http://www.qualys.com/docs/securityalerts/Qadvise-Microsoft-WINS-20040210.pdf>

Microsoft セキュリティ速報 [MS04-006]

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/ms04-007.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

アタックテストサービスエクスプレス カスタマサポート担当

Mail : qualys-support@support.fujitsu.com

電話 : 044-754-3353

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