

平成 15 年 9 月 11 日
富士通株式会社

Qualys 社からの MS DCOM RPCSS 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。

本日、Qualys 社より発信されましたアラートメールにつきまして、ご報告いたします。
この度、マイクロソフト社から、Microsoft Windows DCOM RPCSS サービスにおける、バッファオーバーランの脆弱性および サービス不能(DoS)の脆弱性が報告されました。本脆弱性について、不正なコードを実行されたり、RPCSS サービスを停止される危険性があります。

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

[差出人] Qualys <Qualys@Qualys.com>

[表題] Security Alert: New Microsoft DCOM RPCSS Service Vulnerability

[主な内容]

RPC DCOM のバッファオーバーフローの脆弱性の説明
QualysGuard による、RPC DCOM に特化したチェック方法

[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"の "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「68522」として"Search"し、QualysID「68522」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」ポートを選択します。
もしオーバーHTTP可能なDCOMをご使用の際には、HTTPのポートも選択してください。

- "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]

Microsoft 社

「RPCSS サービスのバッファ オーバーランによりコードが実行される (824146) (MS03-039)」

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS03-039.asp>

Cert Advisory

<http://www.cert.org/advisories/CA-2003-23.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