

平成 16 年 5 月 7 日
富士通株式会社

Sasser ワームについて

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、Sasser ワームに関する情報が 5 月 3 日 付けで Qualys 社より報告されました。
下記の方法にて、QualysGuard で Sasser ワームに利用される脆弱性、MS04-011 の存在を確認することができます。万が一検出された場合には、至急対処をご検討いただきますようお願い申し上げます。

敬具

記

[Sasser ワームの詳細]

Windows 2000、XP システムは Sasser ワームによる影響を受ける可能性があります。Sasser ワーム は、ランダムに選択した IP 上のポート 445 番に対してスキャンをかけ、Microsoft Security Bulletin MS04-011(2004/04/14 発表)で指摘されている LSASS の脆弱性を利用し、感染を広げます。

Sasser ワームに関する詳細は、以下の情報を参照してください。

- ・ Microsoft Security : Sasser ワームについてのお知らせ
<http://www.microsoft.com/japan/security/incident/sasser.msp>
- ・ 株式会社 シマンテック:
<http://www.symantec.com/region/jp/sarcj/data/w/w32.sasser.worm.html>
- ・ トレンドマイクロ 株式会社:
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_SASSER.A&Vsect=T
- ・ 日本 ネットワークアソシエーツ株式会社:
<http://www.nai.com/japan/security/virS.asp?v=W32/Sasser.worm>

なお、QualysGuard にて、Sasser ワーム自体を以下の脆弱性として検出することが可能です。

QualysID : 1135

「Sasser ワームの検出 (Sasser Worm Detected)」

[MS04-011 について]

QualysID : 90108

「Microsoft Windows における複数の脆弱性 (MS04-011)」

MS04-011 に関する詳細は、以下のマイクロソフト社の情報を参照してください。

・ Microsoft Windows のセキュリティ修正プログラム (835732)

(MS04-011)

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS04-011.asp>

http://www.microsoft.com/japan/security/security_bulletins/ms04-011e.asp

[MS04-011 の確認方法]

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) "Scanned TCP Ports"オプションの"None"を選択し、"Additional"にチェックを入れ、TCP ポート「25,80,135,139,443,445,593」を記入します。
- 3) "Scan Dead Hosts"オプションの"Include dead hosts in scans"をチェックします。
- 4) "Vulnerability Detection"オプションの「Custom」を選択し、"Configure..."をクリックします。
Find を「QID」, within を「All」, containing を「90108」として"Search"し、QualysID「90108」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。

- 5) "Profile 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。

< 詳細な確認方法について >

QualysGuard の Windows Authentication オプションを使用することによって、更に詳細な結果を得ることが可能です。

このオプションを使用しない場合、ご対処いただきました後でも、本脆弱性が Possible Threat として検出されますことを、あらかじめご留意ください。

Windows Authentication の設定方法は、以下をご覧ください。

- 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認証を行なう場合は「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。

このオプションは、Administrator の ID とパスワードを QualysGuard へ登録する必要があります。専用の ID を作成していただくか、本診断終了後に ID とパスワードを変更されることをお勧めいたします。

- 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、市川、松本