TD61-4269
HCVU000000007
2009 年 10 月 19 日
日立電線株式会社

# TCP ソケットに関する脆弱性

1．脆弱性の概要

この問題を利用した実際の攻撃は確認されていませんが、HTTP, telnet または FTP のように TCP プロトコルを用いたサービスを行なっている場合、ウインドウサイズを細工したパケットによる TCP socket stress と呼ばれる手法を使うことで、TCP のソケットに対する負荷を増大させ、サービス不能に陥らせることが可能であることが知られています。

この問題はすでに 2000 年に指摘されていましたが、2009 年にその攻撃の有効性や対策についての情報が公表されました。

2．参考情報

(1) JPCERT-AT-2009-0019
複数製品の TCP プロトコルの脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2009/at090019.txt

3．当社製品への影響

当社製品の本脆弱性に関する影響は下記の通りです。

| 製品名 | OS 名称 | 影響 |
|---|---|---|
| Apresia18000 シリーズ | AMIOS | 本脆弱性に該当します |
| Apresia16000 シリーズ | AMIOS | |
| Apresia8000 シリーズ | ApWare | |
| Apresia6000 シリーズ | ApbWare | |
| Apresia2000,3000,4000,5000,13000 シリーズ | AEOS6,AEOS7,AEOS8 | |
| ApresiaLight | APL-Ware | |
| XGMC シリーズ | - | |
| GMC シリーズ | - | |
| GMX シリーズ | - | |
| eWAVE シリーズ | - | |
| BMC/OMC シリーズ | - | |
| FEMX シリーズ | - | |
| GMA シリーズ | - | |

<備考>

本脆弱性は、TCP の基本仕様(プロトコル仕様)に起因します。そのため、上記製品全てについて本脆弱性が存在します。影響といたしましては、攻撃を受けた際、一時的に装置へのアクセスが不可となることが考えられます。

管理ポートを持つ装置については、管理ポートとユーザポートが完全に分離しているため、
ユーザポート側からの TCP パケットによって本問題が発生することはありません。

4．回避策

ワークアラウンドとしては、信頼できない装置からの TCP パケットをフィルタする装置を導入する方法がございます。本問題により一時的に装置へのアクセスができなくなった場合、要因を排除後、10 分ほど待って再度アクセスしてください。

以上