TD61-5877
HCVU000000015
2014 年 7 月 18 日
日立金属株式会社
電線材料カンパニー
情報システム統括部

# OpenSSL の ECDSA に関する脆弱性(CVE-2014-0076)

1．脆弱性の概要

OpenSSL のモンゴメリ・ラダー（Montgomery ladder）の実装は、特定のスワップ操作が一定時間で動作することを確認しないため、楕円曲線デジタル署名アルゴリズム（ECDSA: Elliptic Curve Digital Signature Algorithm）のワンタイムトークンを取得される脆弱性が存在します。

2．参考情報

OpenSSL のモンゴメリ・ラダーの実装における楕円曲線デジタル署名アルゴリズムのワンタイムトークンを取得される脆弱性
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-001795.html

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。

表 1 ネットワーク装置

| 製品名 | OS 名称 | 影響 |
|---|---|---|
| Apresia26000 シリーズ | AMIOS6 | 本脆弱性に該当しません。 |
| Apresia18000 シリーズ | AMIOS2 | |
| Apresia16000 シリーズ | AMIOS3 | |
| Apresia12000 シリーズ | AMIOS5 | |
| Apresia8000 シリーズ | ApWare | |
| Apresia6000 シリーズ | ApbWare | |
| Apresia13000,15000 シリーズ | AEOS8 | |
| Apresia3000,4000,<br>5000,13000 シリーズ | AEOS7,AEOS6 | |
| ApresiaLight FM シリーズ | APLFMOS | |
| ApresiaLight GM シリーズ | APLGMOS | |
| ApresiaLight シリーズ | APL-Ware | |
| XLGMC シリーズ | - | |
| XGMC シリーズ | - | |
| GMC シリーズ | - | |
| GMX シリーズ | - | |
| eWAVE シリーズ | - | |
| BMC シリーズ | - | |
| GMA シリーズ | - | |

表2 ネットワーク管理システム

| ソフトウェア名 | 影響 |
|---|---|
| HCL Manager Station | 本脆弱性に該当しません。 |
| ApresiaManager | |
| MMRPManager | |
| Command Navigator | |
| ApresiaManager/C | |
| GMXManager | |
| GMAManager | |
| BMCManager | |
| OSWManager | |
| OAM-LB Navigator | |
| BFSManager | |

4. 回避策

特に必要ありません。

以上