2014 年 6 月 27 日
株式会社日立ソリューションズ
ネットワークビジネス部

OpenSSL の脆弱性情報（CVE-2014-0224 他）における対応状況について（第 4 報）

2014 年 6 月 5 日に報告された OpenSSL の脆弱性情報（CVE-2014-0224 他）に関して、2014 年 6 月 27 日時点で判明している弊社リリース済みの Aruba Networks 製品における影響範囲、および対策状況・対策予定について報告いたします。

(1) 対象の脆弱性

- Aruba Networks 製品に影響を及ぼす脆弱性
  - CVE-2014-0224
- Aruba Networks 製品に影響を及ぼさない脆弱性

  下記の脆弱性は、対象となる OpenSSL の機能を Aruba Networks 製品が使用していないか有効としていないため、影響はございません。
  - CVE-2014-0221
  - CVE-2014-0195
  - CVE-2014-0198
  - CVE-2010-5298
  - CVE-2014-3470

(2) CVE-2014-0224 の影響を受けることが確認された、弊社リリース済み Aruba Networks 製品

- ArubaOS 6.3.x.x
- AirWave（全バージョン）
- ClearPass 6.3.x（弊社からは 6.3.2 のみリリース済）

(3) CVE-2014-0224 の影響を受けないことが確認された、弊社リリース済み Aruba Networks 製品

- Aruba Instant OS（全バージョン）

(4) 現在確認中の Aruba Networks 製品

- ArubaOS 5.0.x.x、6.1.x.x、6.2.x.x

(5) 対策状況・対策予定

Aruba Networks からは、CVE-2014-0224 対策版が各製品で以下の通りリリースされております。

- ArubaOS 6.3.1.8　　2014 年 6 月 25 日に弊社リリース済
- AirWave 7.7.12　　2014 年 6 月 27 日に弊社リリース済
- ClearPass 6.3.3　　弊社リリースは未定

  ※弊社では ClearPass 6.3.2（CVE-2014-0224 影響あり）のリリースを既にご案内しておりましたが、お客様へのご提供実績はございません。
  そのため本件の緊急対策としては、ClearPass 6.3.3 のリリース予定はございません。

CVE-2014-0224 の影響を受けることが確認されている Aruba Networks 製品をご利用のお客様は、各対策版へのバージョンアップを推奨いたします。

引き続き弊社サポート製品における該当機器・非該当機器および対策につきましては、新たな情報を確認次第、当サポートサイト（http://enugi.hitachi-solutions.co.jp/aruba/）にて報告いたします。

以上