

OpenSSL の脆弱性情報 (CVE-2014-0224 他) における対応状況について (第3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25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

(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) 対策予定

弊社では ArubaOS 6.3.x.x の対策版として、ArubaOS 6.3.1.8 をリリースいたしました。

ArubaOS 6.3.x.x をご使用のお客様は、ArubaOS 6.3.1.8 へのバージョンアップを推奨いたします。

なお、Aruba Networks 社からは AirWave 及び ClearPass の対策版もリリースされたため、現在、弊社リリースへ向けた準備を進めております。

- AirWave 7.7.12 (CVE-2014-0224 対策版) 2014年6月末に弊社リリース予定です。
- ClearPass 6.3.3 (CVE-2014-0224 対策版) 弊社リリース時期は未定です。

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情報が確認され次第、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