【お知らせ】Wi-Fi の暗号化技術「WPA2」脆弱性対策について

10 月 16 日(米国時間)に報告された Wi-Fi 暗号化技術「WPA2」の脆弱性に関して、Aruba 製品における影響範囲および対策についてご連絡いたします。

記

[改訂履歴]
2017/10/23：次の修正版ソフトウェアが追加されましたのでお知らせします。
- Aruba AirMesh MSR シリーズ用修正版追加
- InstantOS パッチ追加

1. WPA2 の脆弱性について

本脆弱性は、Wi-Fi で標準的に用いられる WPA2 鍵管理の欠陥により、攻撃者が WPA2 暗号化ネットワーク上でフレームの復号化、リプレイ、偽造を実行できる場合があると報告されています。これは、暗号鍵を取得してインストールするために Wi-Fi サプリカント（クライアント）と AP（オーセンティケータ）の間で使用される異なる鍵ハンドシェイクに関連しており、ハンドシェイクメッセージのキーイングが再送信されると、さまざまな実装が異なる方法で応答します。これらの応答の一部は、再送が単なるパケット損失だけではなく外部からの攻撃も含まれることがわかりました。

本脆弱性は WPA2 プロトコル実装上の欠陥に関連しており、ハードウェアや設定を変更することなくソフトウェアの更新によって対応頂けることが判明しております。

2. 該当する Aruba 製品

ハードウェアに関わらず、以下の Aruba ソフトウェアバージョンが本脆弱性に該当します。

- ArubaOS (all versions prior to 6.3.1.25)
- ArubaOS 6.4 prior to 6.4.4.16
- ArubaOS 6.5.0.x
- ArubaOS 6.5.1 prior to 6.5.1.9
- ArubaOS 6.5.2.x
- ArubaOS 6.5.3 prior to 6.5.3.3
- ArubaOS 6.5.4 prior to 6.5.4.2
- ArubaOS 8.x prior to 8.1.0.4
- Aruba Instant (all versions prior to 4.2.4.9)
- Aruba Instant 4.3 prior to 4.3.1.6
- Aruba Instant 6.5.2 and 6.5.3 prior to 6.5.3.3
- Aruba Instant 6.5.4 prior to 6.5.4.2
- Clarity Engine 1.0
- HP 501 Wireless Client Bridge prior to 1.0.1.3
- Aruba 501 Wireless Client Bridge prior to 2.0.0.1
- Aruba AirMesh MSR series (all versions)

[脆弱性の影響を受けるケース]
- ✓ ArubaOS AP：Mesh 機能を使用している場合もしくは 802.11r が有効になっている場合
- ✓ InstantOS：Mesh 機能または Wi-Fi Uplink 機能を使用している場合もしくは 802.11r が有効になっている場合
- ✓ Clarity Engine：本脆弱性の影響を受けます。(Airwave 単体の Clarity Live 機能は本脆弱性の影響を受けません)
- ✓ Aruba 501 クライアントブリッジ：本脆弱性の影響を受けます。
- ✓ Aruba AirMesh MSR シリーズ：本脆弱性の影響を受けます。

但し、ArubaOS と InstantOS は オーセンティケータとして動作(すなわち通常の AP 動作モード)且つ 802.11r

が無効である場合、上記の脆弱性の影響を受けません。
　また、HPE MSM シリーズコントローラおよび HPE 8xx Unified WLAN アプライアンスシリーズ製品についても同様に、上記の脆弱性の影響を受けません。

3.　対策

　Aruba では影響を受けるソフトウェアバージョンの修正版をリリースしており、これらのバージョンにアップグレード頂くことを推奨いたします。

- ArubaOS 6.3.1.25
- ArubaOS 6.4.4.16
- ArubaOS 6.5.1.9
- ArubaOS 6.5.3.3
- ArubaOS 6.5.4.2
- ArubaOS 8.1.0.4
- Aruba Instant 4.1.3.5
- Aruba Instant 4.2.4.9
- Aruba Instant 4.3.1.6
- Aruba Instant 6.5.3.3
- Aruba Instant 6.5.4.2
- Clarity Engine 1.0.0.1
- AirMesh MeshOS 4.7.0.4.

上記のソフトウェアは、http://support.arubanetworks.com　からダウンロード入手可能です。
また、ArubaOS/InstantOS については、AP インフラ側で 802.11r を無効化することで、事実上クライアントデバイス側の 802.11r 脆弱性を回避できます。しかしながら、クライアントデバイス側の 4-way ハンドシェイク脆弱性は回避できません。802.11r を無効化する設定は、以下の日本語フォーラムにございます。
ご参考：http://community.arubanetworks.com/t5/日本語フォーラム/11r の無効化/td-p/310220

- HP 501 Wireless Client Bridge V1.0.1.3-HP501-B0012
- Aruba 501 Wireless Client Bridge V2.0.0.1-Aruba501-B0013

上記のソフトウェアは、HPE My Networking ポータルサイトからダウンロード入手可能です。

今後もアップデート情報がある場合には、次のセキュリティアドバイザリでご案内いたします。

セキュリティアドバイザリ：http://www.arubanetworks.com/support-services/security-bulletins/

　今回の脆弱性報告は、現在の Wi-Fi 暗号化通信において多く活用されている WPA2 の脆弱性であったことからネット上の様々な情報ソースにおいて WPA2 をサポートする大半の機器に影響が及ぶ等、様々な情報が展開されていることと思います。
　ただしながら、上記にご案内しましたように、全てのケースにおいて、コントローラ、Instant AP のファームウェアアップグレードが必要なわけではございません。現在では、対策用のソフトウェアも提供しておりますので適宜対応頂き、加えてお客様がご利用されているクライアントデバイスのアップデートもあわせて適用いただき、引続き、無線 LAN ネットワークを安心してご活用頂ければと存じます。

以上