Wi-Fi Protected Access II(WPA2)ハンドシェイクに関する脆弱性について

2018年02月05日
株式会社コレガ

平素は株式会社コレガならびに弊社製品をご愛顧賜り、誠にありがとうございます。

KRACKs」WPA2脆弱性に関する弊社製品の対応状況につきまして、ご案内させていただきます。
以下に、対応状況が明確になっている弊社製品について掲載しております。

○脆弱性の概要

Wi-Fi Protected Access II (WPA2) において、複数の脆弱性が存在します。
主に端末側の脆弱性ですが、一部、AP 側に関連する脆弱性も含まれます。

○対象製品

1.該当製品

CG-WLA300ND
CG-WLA300NEX
CG-WLA300AEX
CG-WLUSB300NS
CG-WLUSB300N
CG-WLCVR300ND

2.非該当製品

CG-WGR1200
CG-WFR600
CG-WLR300NX
CG-WLCVR300NX

○影響

WPA2 を使用して接続した機器間で、パケットの復号や、TCP コネクションのハイジャックなどにより、送受信されている情報が漏洩する可能性があります。

○該当製品への対策（回避策）

・CG-WLA300ND

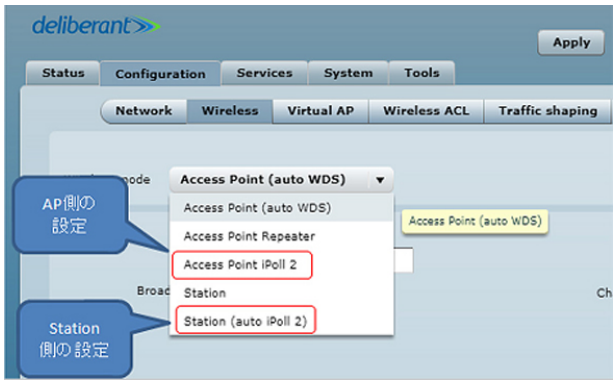
以下の回避策についてご検討をお願い致します。

対策1.
本製品のWDS機能は使用しないでください。
操作画面内の【WDS設定】から、WDSモードで『DISABLE』を選択します。（初期値『DISABLE』）

・CG-WLA300NEX
・CG-WLA300AEX

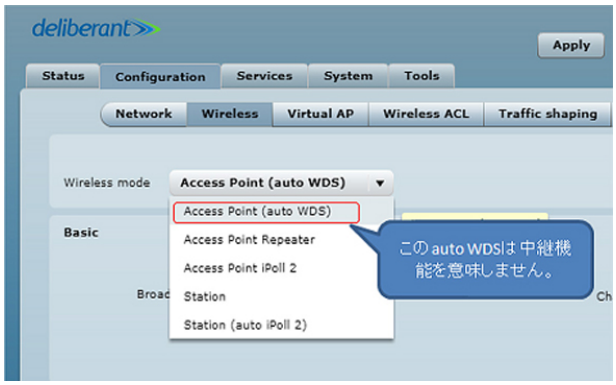
以下いずれかの回避策についてご検討をお願い致します。

対策1.
無線ブリッジ環境において、独自プロトコルであるiPollを利用した通信を行う。
※CG-WLA300NEX、もしくはAEX同士の接続に限定されます。



※画面はCG-WLA300AEXのものとなります。
CG-WLA300NEXではそれぞれ「Access Point iPoll」「Station (auto iPoll)」と表示されます。

対策2.
単体のアクセスポイントとして動作させる。
※クライアント機器には本脆弱性の対策がなされている必要があります。



対策3.
無線機器間の通信を行う際、上位のレイヤーのプロトコル等（VPN、HTTPS）を利用して通信を暗号化する。

- **CG-WLUSB300N**
- **CG-WLUSB300NS**
- **CG-WLCVR300ND**

以下の回避策についてご検討をお願い致します。

対策1.
CG-WLUSB300N、CG-WLUSB300NS、及びCG-WLCVR300NDの使用を停止してください。
なお、CG-WLUSB300N、CG-WLUSB300NS、及びCG-WLCVR300NDのサポートサービス期間は終了しております。

○補足：参考資料

- **情報処理推進機構**
  WPA2 における複数の脆弱性について
  https://www.ipa.go.jp/security/ciadr/vul/20171017_WPA2.html

- **無線LANビジネス推進連絡会【WiBiz（ワイビズ）】**
  無線LAN（Wi-Fi）暗号化における脆弱性への対応について
  http://www.wlan-business.org/archives/11325

以上