CG-WGR1200における複数の脆弱性について

2018年03月09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。

○問題の概要

対象製品には、以下の脆弱性が存在します。

・バッファオーバーフロー
・OSコマンドインジェクション
・認証不備

このため、次のような影響を受ける可能性があります。

・当該製品にアクセス可能な第三者によって、任意のコードを実行される。
・当該製品にアクセス可能な第三者によって、任意のOSコマンドを実行される。
・当該製品にアクセス可能な第三者によって、ログインパスワードを変更される。結果として、管理画面にログインされ、当該製品の設定変更等、任意の操作が行われる。

○当社製品

1.該当製品

下記製品は、複数の脆弱性が存在します。

無線LANルータ
CG-WGR1200 ファームウェア Ver. 2.20 およびそれ以前

2.対策

以下のいずれかの方法で回避してください。

(1)CG-WGR1200の使用を停止してください。
なお、CG-WGR1200のサポートサービス期間は終了しております。

(2)回避策を適用する
CG-WGR1200のサポートサービス期間は終了しているため、対策版ファームウェアのリリース予定はありませんが、当該製品を引き続き使用される場合には、以下の回避策を適用することにより、脆弱性による影響を軽減してください。
・第三者が外部から当該製品にアクセスできないよう、リモートアクセス機能を無効にする。
・LAN内から当該製品に対する不正なアクセスをさせないようにする。

○補足：CG-WGR1200における複数の脆弱性 関連サイト
・JVN
http://jvn.jp/jp/JVN15201064/

以上