CG-WLR300NXの複数の脆弱性について

2016年 11月11日
株式会社コレガ

○問題の概要

対象製品には、以下の脆弱性が存在します

1)アクセス制限不備の脆弱性
対象製品には、アクセス制限不備の脆弱性が存在します。
この為、当該製品にアクセス可能な第三者によって、管理者がログインしている当該製品上で任意の操作を実行される可能性があります。

2)クロスサイトリクエストフォージェリの脆弱性
対象製品には、クロスサイトリクエストフォージェリの脆弱性が存在します。
この為、当該製品にログインした状態で、細工されたページにアクセスした場合、意図しない操作をさせられる可能性があります。

3)クロスサイトスクリプティングの脆弱性
対象製品には、クロスサイトスクリプティングの脆弱性が存在します。
この為、当該製品にログインした状態のユーザのウェブブラウザ上で、任意のスクリプトを実行される可能性があります。

○当社製品

1)該当製品

＜無線LANルータ＞
CG-WLR300NX ファームウェア Ver. 1.20 およびそれ以前

2)対策
現在公開している最新ファームウェアにて問題点に対する対策を実施しておりますので、ファームウェアの更新をお願いします。

・CG-WLR300NX ファームウェア Ver.1.30以降
https://www.allied-telesis.co.jp/products/list/corega/discontinued-products/

○補足：CG-WLR300NXの複数の脆弱性について　関連サイト

・JVN:
http://jvn.jp/jp/JVN23549283/
http://jvn.jp/jp/JVN23823838/
http://jvn.jp/jp/JVN92237169/

以上