弊社製 **HEMS** におけるセキュリティ脆弱性について

2024 年 1 月 30 日

シャープ株式会社

平素は、シャープのクラウド連携エネルギーコントローラをご愛用いただき、誠にありがとうございます。

この度、弊社が販売しているクラウド連携エネルギーコントローラに関しまして、セキュリティ上の脆弱性が存在することがわかりました。脆弱性の概要、対象製品につきましては、下記の表をご覧ください。

当該製品をご愛用いただいておりますお客様に多大なご迷惑をおかけしますことを深くお詫び申し上げます。

脆弱性識別番号	JVNVU#94591337
該当する製品名およびバージョン	製品名：クラウド連携エネルギーコントローラ(機器連携コントローラ) 機種名：JH-RVB1 /JH-RV11 バージョン：Ver.B0.1.9.1 以前
攻撃が行われる条件	本脆弱性を利用した攻撃が成立するためには、攻撃起点となるコンピュータが当該製品と同一のネットワークに接続されていることが条件となります。上記以外のケースにおいては、本脆弱性による影響はありません。
発生しうる影響	悪意のある攻撃者により、当該製品の設定情報やお客様宅の電力情報等が漏洩、または、当該製品の設定情報を不正に変更される、当該製品を踏み台にしたサイバー攻撃の起点になるおそれがあります。
影響軽減策	当該製品をお使いのお客様の環境において、当該製品は直接インターネットに接続せず、必ずルーター等で保護されたネットワーク内で使用してください。無線 LAN ルーターをお使いの場合は、強固な暗号化方式（WPA2 パーソナル（AES）以降を推奨）を設定する、管理用パスワードを初期状態から変更する、ファームウェアを最新の状態に保つ、等の対策を実施してください。古い暗号化方式にしか対応していない無線 LAN ルーターのご使用は推奨されません。 同一のネットワークに接続するパソコンがある場合は、OS の定期的なアップデートを実施するとともに、セキュリティ対策ソフトを入れ、その定義ファイルを最新の状態に保ってください。これらの対応で、上記の影響を被るリスクを低減することができます。
対応方法	クラウド連携エネルギーコントローラがインターネットに接続されている環境においては、自動でバージョンアップされます。本脆弱性対策後のファームウェア・バージョンは Ver.B0.2.0.0 以降となります。 本件に関するお問い合わせ シャープ（株） お客様相談室 https://jp.sharp/support/taiyo/

謝辞	本脆弱性は、JPCERT/CC 様経由で GMO サイバーセキュリティ by イエラエ株式会社 馬場将次様のご報告により発見されました。 ご報告に対し、謹んで感謝申し上げます。
情報	**JVNVU#94591337**