エコガイド TAB における情報漏えいの脆弱性並びに情報漏えい、情報改ざん及びサービス拒否(DoS)の脆弱性

公開日 2025 年 7 月 10 日
最終更新日 2025 年 9 月 18 日
三菱電機株式会社

■概要

三菱太陽光発電システム用モニターのエコガイド TAB(2015 年生産終了、2020 年保守サポート終了)において、不十分なパスワード強度(CWE-521[1])による情報漏えいの脆弱性並びにハードコードされた認証情報の使用(CWE-798[2])による情報漏えい、情報改ざん及びサービス拒否(DoS)の脆弱性が存在することが判明しました。当該製品のユニット間(計測ユニット・表示ユニット間)の Wi-Fi 通信の通信エリア内(10m 程度)に侵入した攻撃者は、SSID からパスワードを算出することができる可能性があります(CVE-2025-5022)。さらに、同脆弱性(CVE-2025-5022)を悪用するなどし、ユニット間の Wi-Fi 通信に侵入した攻撃者はハードコーディングされた製品シリーズ共通のユーザ ID とパスワードを使用し、当該製品に保持されている発電電力、売電電力等の情報を窃取したり、当該製品に保持又は設定されている情報を改ざん・破壊したり、当該製品をサービス停止(DoS)状態に陥らせたりすることができる可能性があります(CVE-2025-5023)。

また、当該製品で個別エアコン操作の機能が使用できるように設定されている場合には、CVE-2025-5022 の脆弱性を悪用してユニット間の Wi-Fi 通信に侵入した攻撃者が、ECHONET Lite[3]のコマンドを実行することによって、エアコンの運転 ON/OFF、設定温度の変更等の個別エアコン操作を実行できる可能性があります。

これらの脆弱性の影響を受ける製品名を以下に示しますので、当該製品の使用中止又は軽減策の実施をお願いいたします。

なお、当該製品が接続されているパワーコンディショナ、接続箱、太陽電池モジュール等の発電機能に関連する機器は、この脆弱性の影響を受けません。また、当該製品が保持している情報に個人情報等の機微な情報はありません。

■CVSS スコア [4]

CVE-2025-5022 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値:6.5
CVE-2025-5023 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H 基本値:7.1

■該当製品の確認方法

下記製品の全てのバージョンが影響を受けます。

PV-DR004J
PV-DR004JA

但し、個別エアコン操作の機能があるのは、表示ユニット Ver.02.00.01 以降のバージョン及び計測ユニット Ver.02.03.01 以降のバージョンです。

■脆弱性の説明

三菱太陽光発電システム用モニターのエコガイド TAB において、以下の脆弱性が存在します。

・CVE-2025-5022: 不十分なパスワード強度(CWE-521)による情報漏えいの脆弱性
・CVE-2025-5023: ハードコードされた認証情報の使用(CWE-798)による情報漏えい、情報改ざん及びサービス拒否(DoS)の脆弱性

■脆弱性がもたらす脅威

当該製品のユニット間(計測ユニット・表示ユニット間)の Wi-Fi 通信の通信エリア内に侵入した攻撃者は、SSID からパスワードを算出することができる可能性があります。さらに、同脆弱性を悪用するなどし、ユニット間の Wi-Fi 通信に侵入した攻撃者は、ハードコーディングされた製品シリーズ共通のユーザ ID とパスワードを使用し、当該製品に保持されている発電電力、売電電力等の情報を窃取したり、当該製品に保持又は設定されている情報を改ざん・破壊したり、当該製品をサービス停止(DoS)状態に陥らせたりすることができる可能性があります。

また、当該製品で個別エアコン操作の機能を使用できるように設定されている場合には、CVE-2025-5022 の脆弱性を悪用してユニット間の Wi-Fi 通信に侵入した攻撃者が、ECHONET Lite のコマンドを実行することによって、エアコンの運転 ON/OFF、設定温度の変更等の個別エアコン操作を実行できる可能性があります。

なお、当該製品が接続されているパワーコンディショナ、接続箱、太陽電池モジュール等の発電機能に関連する機器は、この脆弱性の影響を受けません。また、当該製品が保持している情報に個人情報等の機微な情報はありません。

---

1 https://cwe.mitre.org/data/definitions/521.html
2 https://cwe.mitre.org/data/definitions/798.html
3 ECHONET Lite はエコーネットコンソーシアムの商標です。
4 https://www.ipa.go.jp/security/vuln/CVSSv3.html

■対策方法

該当製品の保守サポートは終了しておりますので、使用中止又は軽減策の実施をお願いいたします。
使用を継続されるお客様は、軽減策を実施ください。
使用を中止されるお客様は、個別エアコン操作の機能をご使用されている場合と、ご使用されていない場合で、中止方法が異なりますので、以下示す使用中止方法に従ってください。

・個別エアコン操作の機能を使用していないお客様の場合
当該製品の計測ユニットと表示ユニットの電源を OFF にしてください。
・個別エアコン操作の機能を使用しているお客様の場合
当該製品の個別エアコン操作の機能が使用できないように、当該製品の表示ユニットの設定を変更したうえで、計測ユニットと表示ユニットの電源を OFF にしてください。さらに、取扱説明書を参照いただき、当該製品に接続設定されている中継器と無線 LAN アダプターを初期化してください。
個別エアコン操作の設定変更後のエアコン操作は、エアコンに附属のリモコンで実施いただくようお願いいたします。

■軽減策

これらの脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。

・悪意のある攻撃者になりうる第三者による当該製品の Wi-Fi 通信エリア内への侵入を、防止してください。

■謝辞

本脆弱性をご報告いただいた、矢野 礼伊様に感謝いたします。

■お客様からのお問い合わせ先

三菱太陽光発電技術相談センター
電話番号：0120－314－382(無料)
お問い合わせ用メールアドレス：taiyo@nm.MitsubishiElectric.co.jp
受付時間：9：00～12：00、13：00～17：00(土日祝日・当社休業日除く)

■更新履歴

2025 年 9 月 18 日
・「概要」、「該当製品の確認方法」、「脆弱性がもたらす脅威」、「対策方法」及び「軽減策」を改訂しました。