IEEE802.11 規格のフラグメンテーションに関する複数の脆弱性（FragAttacks）

公開日 2021 年 9 月 2 日
最終更新日 2022 年 5 月 10 日
三菱電機株式会社

■概要

IEEE802.11 規格のフレームアグリゲーションやフラグメンテーションにおける設計上の欠陥に起因する複数の脆弱性が、公開されました。この脆弱性を悪意のある攻撃者に悪用された場合、対象製品において、通信内容を窃取されたり不正なパケットが挿入される可能性があります。本脆弱性の影響を受ける製品名を以下に示しますので、対策又は軽減策・回避策の実施をお願いいたします。

■CVSS スコア

CVE-2020-24586: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N 基本値:3.5
CVE-2020-24587: CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N 基本値:2.6
CVE-2020-24588: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N 基本値:3.5
CVE-2020-26139: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:5.3
CVE-2020-26140: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値:6.5
CVE-2020-26142: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値:7.5
CVE-2020-26143: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値:6.5
CVE-2020-26144: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値:6.5
CVE-2020-26145: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値:6.5
CVE-2020-26146: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値:5.3
CVE-2020-26147: CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:N 基本値:5.4

■脆弱性の説明

IEEE802.11 規格に関する複数の脆弱性(Frag Attacks)が発見されました。当社製品は、これらの脆弱性の内、下記脆弱性の影響を受ける可能性があります。**「■影響を受ける製品、対策方法及び軽減策・回避策」に、製品毎に影響を受ける可能性がある脆弱性の番号(1～11)を掲載しますので、ご確認ください。**

1. ネットワークの再接続時にメモリからフラグメントのキャッシュがクリアされないことにより、特定の状況下において攻撃者にパケットの内容を窃取される脆弱性（CVE-2020-24586）（CWE-212）
2. 異なる鍵で暗号化されたフラグメント化されたフレームを再構成してしまうことにより、特定の状況下において攻撃者にパケットの内容を窃取される脆弱性（CVE-2020-24587）（CWE-326）
3. ヘッダ中のフレームアグリゲーションフラグが保護されていないため、攻撃者によりヘッダ情報を書き換えられ、不正なパケットが挿入される脆弱性（CVE-2020-24588）（CWE-306）
4. 送信者が認証されていない場合でも EAPOL フレームを転送してしまう脆弱性（CVE-2020-26139）（CWE-287）
5. 保護されたネットワークにおいて、平文のデータフレームを受け入れてしまう脆弱性（CVE-2020-26140）（CWE-74）
6. フラグメント化されたフレームをフルフレームとして処理してしまう脆弱性（CVE-2020-26142）（CWE-74）
7. 保護されたネットワークにおいて、フラグメント化された平文のデータフレームを受け入れてしまう脆弱性（CVE-2020-26143）（CWE-20）
8. 暗号化されたネットワークにおいて、EtherType に EAPOL が指定された RFC1042 ヘッダを持つ、平文の A-MSDU フレームを受け入れてしまう脆弱性（CVE-2020-26144）（CWE-20）
9. 暗号化されたネットワークにおいて、フラグメント化された平文のブロードキャストフレームをフルフレームとして受け入れてしまう脆弱性（CVE-2020-26145）（CWE-20）
10. 連続しないパケット番号を持つ暗号化されたフラグメントをリアセンブルしてしまう脆弱性（CVE-2020-26146）（CWE-20）
11. 暗号化されたフラグメントと平文のフラグメントを混合してリアセンブルしてしまう脆弱性（CVE-2020-26147）（CWE-74）

■脆弱性がもたらす脅威

これらの脆弱性により、フレームアグリゲーションやフラグメンテーションの際に、攻撃者によって不正なパケットが挿入されたり、通信内容が窃取されたりする可能性があります。

■影響を受ける製品、対策方法及び軽減策・回避策

[1]【太陽光発電システム カラーモニター エコガイド】

型番	対策及び軽減策・回避策
PV-DR006L-SET-M PV-DR006L-IFU-GW-M PV-DR006L-IFU-MRC-M 影響を受ける製品は上記製品同梱の計測ユニットで全てのバージョンです （3、5の影響を受ける可能性があります） PV-DR006L-SET-M PV-DR006L-SET-Y PV-DR006L-IFU-GW-M PV-DR006L-IFU-GW-Y 影響を受ける製品は上記製品同梱の情報収集ユニットで全てのバージョンです （1、2、3、4、5、7、8、9、10、11の影響を受ける可能性があります）	〈想定される影響〉 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ 計測ユニットは、据付工事説明書に従い、情報収集ユニットに接続してご使用下さい。 情報収集ユニットには計測ユニット以外の無線機器を接続しないでください。ただし、三菱HEMS（HM-ST03 タブレット用）アプリをご利用の場合は、HEMS 製品とその操作用端末（タブレット）も情報収集ユニットに接続できます。 情報収集ユニットをインターネットに接続する場合はルーターを介して接続してください。 情報収集ユニットに無線 LAN イーサネットコンバータを接続して無線 LAN でご使用の場合、及び情報収集ユニットをルーターに接続してご使用の場合は、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 また同ネットワーク内でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先

三菱電機お客さま相談センター　0120-139-365(無料)　携帯・PHS　0570-077-365(有料)

フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[2]【HEMS 対応アダプター・無線 LAN アダプター】

型番	対策及び軽減策・回避策
HEMS 対応アダプター: GT-HEM1 GT-HEM2 GT-HEM3 GT-HEM3-M P-01HMA P-HM02WA P-HM03WA VEZ-HM01WA HM-01A-CS HM-01A-EX HM-01A-VEH HM-02A-CS HM-02A-REF HM-02A-VEH HM-WF001 HM-W002-AC HM-W002-ACB 無線 LAN アダプター:: MAC-884IF MAC-888IF 影響を受ける製品は上記製品の全てのバージョンです（3、5の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)
フリーダイヤル, ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[3]【ルームエアコン】

型番	対策及び軽減策・回避策
MSZ-EM22/25/28/36/40/56/63/71/80E2(S) MSZ-EM22/25/28/36/40/56/63/71/80/90E3(S) 影響を受ける製品は上記製品の全てのバージョンです（3、5の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)
フリーダイヤル, ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[4]【IHクッキングヒーター】

型番	対策及び軽減策・回避策
CS-PT31HNWSR-H G32MS-H G32M-H 影響を受ける製品は上記製品の全てのバージョンです （3、5の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[5]【三菱 HEMS 用　エネルギー計測ユニット】

型番	対策及び軽減策・回避策
HM-EM02 HM-EM03-W 影響を受ける製品は上記製品の全てのバージョンです （3、5の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・エネルギー計測ユニットをインターネットに接続される場合は、直接ルーターへは接続せず、情報収集ユニットを介して接続ください。HM-EM02 は情報収集ユニット HM－GW02 に接続し、HM-EM03-W は情報収集ユニット HM-GW03 に接続してください。 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[6]【無線 LAN アダプター】

型番	対策及び軽減策・回避策
MAC-895IF 影響を受ける製品は上記製品の全てのバージョンです（2、3、6、8、9、10の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先

三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)

フリーダイヤル, ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[7]【ルームエアコン・無線 LAN アダプター】

型番	対策及び軽減策・回避策
ルームエアコン: MSZ-FD40/56/63/71/8022S MSZ-HXV25/28/40/56/63/71/8022S MSZ-VXV40/56/63/71/8022S MSZ-ZD25/28/40/56/63/71/8022(S) MSZ-FZ40/56/63/71/80/9021S MSZ-ZW22/25/28/36/40/56/63/71/80/9021(S) MSZ-FZV40/56/63/71/80/9021S MSZ-ZXV22/25/28/36/40/56/63/71/80/9021(S) MSZ-EM22/25/28/36/40/56/63/71/80/9021E9(S) MSZ-FZ40/56/63/71/80/9020S MSZ-ZW22/25/28/36/40/56/63/71/80/9020(S) MSZ-FZV40/56/63/71/80/9020S MSZ-ZXV22/25/28/36/40/56/63/71/80/9020(S) MSZ-EM22/25/28/36/40/56/63/71/80/9020E8(S) 無線 LAN アダプター: MAC-900IF PAC-SK43ML 影響を受ける製品は上記製品のバージョン 30.00～33.00 です (1、2、3、4、5、7、8、9、10、11の影響を受ける可能性があります)	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 無線 LAN ソフトウェア Ver34.00 以降で対策しております。 「霧ヶ峰 REMOTE」アプリより対策版にアップデートください。 ソフトウェアのバージョン確認およびアップデートは、「霧ヶ峰 REMOTE」アプリの「エアコン管理」-「(部屋名称)」にある「無線 LAN ソフト更新」から行ってください。詳細は以下サイトにある霧ヶ峰 REMOTE 取扱説明書をご覧ください。 https://www.mitsubishielectric.co.jp/home/kirigamine/function/remote/ib.html HEMS のみご使用の場合、バージョン確認およびアップデートするために、霧ケ峰 REMOTE 取扱説明書をご参照のうえ霧ケ峰 REMOTE アプリをインストールして、霧ケ峰 REMOTE を使用できるよう設定ください。 PAC-SK43ML をご使用の場合、以下の軽減策・回避策を実施ください。 ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先

三菱電機お客さま相談センター 0120-139-365(無料) 携帯・PHS 0570-077-365(有料)

フリーダイヤル, ナビダイヤルをご利用いただけない場合 03-3414-9655(有料)

[8]【冷蔵庫】

型番	対策及び軽減策・回避策
MR-MXD50/57G MR-WXD52/60/70G 影響を受ける製品は上記製品のバージョン 00.43 です（1、2、3、4、5、7、8、9、10、11の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 無線 LAN ソフトウェアバージョン Ver00.68 以降で対策しております。 「MyMU」アプリより対策版にアップデートください。 ソフトウェアのバージョン確認およびアップデートは、「MyMU」アプリの「登録機器」にある「アダプター情報」から行ってください。詳細は以下サイトにある無線 LAN アダプターのソフトウェア更新方法（取扱説明書・別冊）をご覧ください。 https://www.mitsubishielectric.co.jp/home/mymu/entry_ib2.html ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先

三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)

フリーダイヤル, ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[9]【HEMS 対応アダプター、無線 LAN アダプター】

型番	対策及び軽減策・回避策
GT-HEM4 GT-RA1 GT-RA2 影響を受ける製品は上記製品のバージョン00.68 以前です （1、2、3、4、5、7、8、9、10、11の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ GT-RA1、GT-RA2 については、アダプターソフトウェアバージョン Ver00.69 以降で対策しております。 「MyMU」アプリ、または「DIAHOT REMOTE」アプリより対策版にアップデートください。 MyMU をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「MyMU」アプリの「登録機器」にある「アダプター情報」から行ってください。詳細は以下サイトにある無線 LAN アダプターのソフトウェア更新方法（取扱説明書・別冊）をご覧ください。 https://www.mitsubishielectric.co.jp/home/mymu/entry_ib2.html DIAHOT REMOTE をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「DAHOT REMOTE」アプリの「機器情報」にある「アダプターソフトウェアバージョン」から行ってください。詳細は以下サイトにある DIAHOT REMOTE 取扱説明書をご覧ください。 https://www.mitsubishielectric.co.jp/home/ecocute/function/remote/ib.html 対策ソフトウェアが無い機種については、軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先

三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)

フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[10]【バス乾燥・暖房・換気システム】

型番	対策及び軽減策・回避策
V-241BZ-RC WD-240DK-RC 影響を受ける製品は上記製品のバージョン00.64 以前です （1、2、3、4、5、7、8、9、10、11の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 無線 LAN アダプターのソフトウェアバージョン Ver00.65 以降で対策しております。 「MyMU」アプリ、または「バスカラット REMOTE」アプリより対策版にアップデートください。 MyMU をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「MyMU」アプリの「登録機器」にある「アダプター情報」から行ってください。詳細は以下サイトにある無線 LAN アダプターのソフトウェア更新方法（取扱説明書・別冊）をご覧ください。 https://www.mitsubishielectric.co.jp/home/mymu/entry_ib2.html バスカラット REMOTE をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「バスカラット REMOTE」アプリの「機器情報」にある「アダプターソフトウエアバージョン」から行ってください。詳細は以下サイトにあるバスカラット REMOTE 取扱説明書をご覧ください。 https://www.mitsubishielectric.co.jp/ldg/ja/air/products/ventilationfan/bath/IB/pdf/bathkaratremote.pdf ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[11]【炊飯器】

型番	対策及び軽減策・回避策
NJ-AWBX10 影響を受ける製品は上記製品のバージョン 00.41 です（1、2、3、4、5、7、8、9、10、11の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 無線 LAN アダプターのソフトウェアバージョン Ver00.75 以降で対策しております。 「MyMU」アプリ、または「WiFi らく楽炊飯」アプリより対策版にアップデートください。 MyMU をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「MyMU」アプリの「登録機器」にある「アダプター情報」から行ってください。詳細は以下サイトにある無線 LAN アダプターのソフトウェア更新方法（取扱説明書・別冊）をご覧ください。 https://www.mitsubishielectric.co.jp/home/mymu/entry_ib2.html WiFi らく楽炊飯をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「WiFi らく楽炊飯」アプリの「機器情報」にある「通信アダプターソフトウエアバージョン」から行ってください。 ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先

三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)

フリーダイヤル, ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[12]【三菱 HEMS 用　制御アダプター】

型番	対策及び軽減策・回避策
P-HM04WA 影響を受ける製品は上記製品のバージョン00.66 以前です （1、2、3、4、5、7、8、9、10、11の影響を受ける可能性があります）	<想定される影響> 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ アダプターソフトウェアバージョン Ver00.67 以降で対策しております。 バージョン Ver00.66 以前は、軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655（有料）

[13]【三菱 HEMS 用　情報収集ユニット】

型番	対策及び軽減策・回避策
HM-GW02 HM-GW02MJ HM-GW03 HM-GW03MJ 影響を受ける製品は上記製品の全てのバージョンです （1、2、3、4、5、7、8、9、10、11の影響を受ける可能性があります）	＜想定される影響＞ 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・情報収集ユニットをインターネットに接続する場合はルーターを介して接続してください。 ・情報収集ユニットには HEMS 製品以外の無線機器を接続しないでください。ただし、三菱 HEMS（HM-ST03 タブレット用）アプリ(注1)をご利用の場合はその操作用端末（タブレット）も情報収集ユニットに接続できます。 （注1） HM-GW02 をご使用の場合は三菱 HEMS（HM-ST02）アプリ HM-GW02MJ をご使用の場合は三菱地所ホーム HEMS ver.2 アプリ HM-GW03MJ をご使用の場合は三菱地所ホーム HEMS ver.3（タブレット用）アプリ 無線ルーターの設定について、以下をご確認ください（情報収集ユニットを除く）。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[14]【表示器 GOT 用 無線 LAN 通信ユニット】

型番	対策及び軽減策・回避策
GT25-WLAN （GOT2000 シリーズ GT25、GT27 モデルに GT25-WLAN を装着した構成） 影響を受ける製品は上記製品のシステムアプリケーション(拡張機能)「無線 LAN」バージョン 01.39.000 以前です （1、2、3、5、7、8、10の影響を受ける可能性があります）	＜想定される影響＞ 悪意のある攻撃者に脆弱性を悪用された場合、通信内容の窃取や不正パケットの挿入等の影響を受ける可能性があります。 ＜対策＞ 該当製品/バージョンをご使用のお客様は、以下に示す手順に従って対策バージョンに更新してください。 バージョン確認方法 バージョン確認方法については、以下のマニュアルを参照してください。 なお、最新のマニュアルを、三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)のマニュアルダウンロードコーナーよりダウンロードできます。 GOT2000 シリーズ本体取扱説明書(ユーティリティ編)(SH-081187) 「6.9 章パッケージ管理」内の「プロパティ操作」 対策バージョン システムアプリケーション(拡張機能)「無線 LAN」バージョン:01.45.000 以降 (GT Designer3 Version1(GOT2000) Ver.1.275M 以降に同梱されています。) CVE-2020-26146 (脆弱性の説明 10)に対する対策は含まれません。軽減策・回避策を実施されることを推奨いたします。 更新手順 1. 三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)のソフトウェアダウンロードコーナーより、最新の GT Designer3 Version1(GOT2000)をダウンロードし、インストーラのメッセージに従いパソコンにインストールしてください。 2. 該当製品で使用しているプロジェクトデータを GT Designer3 Version1(GOT2000)で開きます。 3. [通信]→[GOT への書込み]メニューを選択し、パッケージデータを GOT 本体へ転送してください。転送に関する詳細な手順は、以下のマニュアルを参照してください。なお、最新のマニュアルを、三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)のマニュアルダウンロードコーナーよりダウンロードできます。 GT Designer3 (GOT2000) 画面設計マニュアル(SH-081219) 「4 章 GOT と通信する」 4. 前述のバージョン確認方法に従い、対策バージョンとなっていることを確認してください。 ＜軽減策・回避策＞ 無線 LAN 通信ユニットをアクセスポイントとしてご使用する場合、無線 LAN 通信ユニットの設定について、以下をご確認ください。 ・無線 LAN 設定に使用するパスフレーズは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくいものをご使用ください。 ・無線 LAN 設定のセキュリティ認証方式は WPA あるいは WPA2 を使用してください。 ・IP フィルタ機能※1を使用し、接続可能な IP アドレスを適切に制限してください。 ※1:GT Designer3 (GOT2000)画面設計マニュアル(SH-081219)「5.4.3 章 IP フィルタを設定する」を参照ください。 無線 LAN 通信ユニットをステーションとしてご使用する場合、無線 LAN ルータの設定について、以下をご確認ください。 ・無線 LAN 設定に使用するパスフレーズは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくいものをご使用ください。 ・無線 LAN 設定のセキュリティ認証方式は WPA あるいは WPA2 を使用してください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなどインターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。無線 LAN の設定については無線 LAN ルーターのメーカーにお問い合わせください。 また同ネットワーク内でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・OS、ソフトウェア、ウィルス対策ソフトなどを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
お客様からのお問い合わせ先につきましては、製品をご購入いただいた弊社の支社、代理店にご相談ください。

〈お問い合わせ | 三菱電機 FA〉
https://www.mitsubishielectric.co.jp/fa/support/purchase/index.html

■更新履歴
2022 年 5 月 10 日
影響を受ける製品において、下記の製品のバージョン情報や対策方法の情報を追加
[14]【表示器 GOT 用 無線 LAN 通信ユニット】 GT25-WLAN

2022 年 3 月 22 日
影響を受ける製品を追加し、想定される影響と対策情報を記載
[14]【表示器 GOT 用 無線 LAN 通信ユニット】 GT25-WLAN

2022 年 1 月 19 日
影響を受ける製品を追加し、想定される影響と対策情報を記載
[1]【太陽光発電システム カラーモニター エコガイド】 機種追加
PV-DR006L-SET-M、PV-DR006L-SET-Y、PV-DR006L-IFU-GW-M、PV-DR006L-IFU-GW-Y（情報収集ユニット）
[13]【三菱 HEMS 用 情報収集ユニット】
HM-GW02、HM-GW02MJ、HM-GW03、HM-GW03MJ

2021 年 11 月 30 日
影響を受ける製品において、下記の製品のバージョン情報や対策方法の情報を追加
[7]【ルームエアコン・無線 LAN アダプター】 PAC-SK43ML
[8]【冷蔵庫】 MR-MXD50/57G、MR-WXD52/60/70G
[9]【HEMS 対応アダプター、無線 LAN アダプター】 GT-HEM4、GT-RA1、GT-RA2
[10]【バス乾燥・暖房・換気システム】 V-241BZ-RC、WD-240DK-RC
[11]【炊飯器】 NJ-AWBX10
[12]【三菱 HEMS 用 制御アダプター】 P-HM04WA