

複数の家電製品における悪意のあるスクリプトを含んだメッセージを応答する脆弱性及びアクセスポイントモード時のサービス拒否(DoS)の脆弱性

公開日 2022 年 9 月 29 日
最終更新日 2023 年 10 月 26 日
三菱電機株式会社

■概要

三菱電機製の複数の家電製品に、以下の脆弱性が存在することが判明しました。

(1) 悪意のあるスクリプトを含んだメッセージを応答する脆弱性(CVE-2022-33322)

クロスサイトスクリプティング(CWE-79)¹に起因する悪意のあるスクリプトを含んだメッセージを応答する脆弱性が存在します。この脆弱性を悪意のある攻撃者に悪用された場合、当該製品が悪意のあるスクリプトを含んだメッセージを応答することにより、ブラウザ上で悪意のあるスクリプトが実行され、ブラウザ内の情報の漏えい等が発生する可能性があります。

本脆弱性の影響を受ける製品名を次ページ以降に示しますので、対策又は軽減策・回避策の実施をお願いいたします。

なお、本脆弱性により当該製品からの機器データの情報漏えいや、機器の不正操作の影響を受けません。

また、以下の当社家電製品又はご使用環境では、本脆弱性の影響を受けません。

- ・Wi-Fi 接続に対応していない製品
- ・Wi-Fi 接続対応の製品において Wi-Fi 接続を使用していない場合

(2) アクセスポイントモード時のサービス拒否(DoS)の脆弱性(CVE-2022-29859)

アクセスポイントモード時の DHCP 処理において、Realtek 社製通信チップの脆弱性に起因する、解放済みメモリの使用(CWE-416)²による脆弱性が存在します。この脆弱性を Wi-Fi の受信圏内にいる悪意のある攻撃者に悪用された場合、当該製品がサービス拒否(DoS)状態に陥る可能性があります。

アクセスポイントモードは、機器登録の際に用いるモードです。通常のご使用状態では、アクセスポイントモードを使用しないため、本脆弱性の影響を受けません。

本脆弱性の影響を受ける製品名を次ページ以降に示しますので、対策又は軽減策・回避策の実施をお願いいたします。

なお、本脆弱性により個人情報や機器データの情報漏えいや、機器の不正操作の影響を受けません。

また、以下の当社家電製品又はご使用環境では、本脆弱性の影響を受けません。

- ・Wi-Fi 接続に対応していない製品
- ・Wi-Fi 接続対応の製品において Wi-Fi 接続を使用していない場合
- ・Wi-Fi 接続対応の製品において WPS 接続を使用する場合
- ・Wi-Fi 接続対応の製品において機器登録を済ませ通常使用されている場合

■CVSS スコア³

(1) CVE-2022-33322 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N 基本値:6.8

(2) CVE-2022-29859 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L 基本値:3.1

■脆弱性の説明

(1) 悪意のあるスクリプトを含んだメッセージを応答する脆弱性(CVE-2022-33322)

三菱電機製の家電製品には、Web サーバにおける入力内容のフィルタリング/検証/特殊な文字の無効化が不十分であり、クロスサイトスクリプティング(CWE-79)に起因する悪意のあるスクリプトを含んだメッセージを応答する脆弱性(CVE-2022-33322)が存在します。

(2) アクセスポイントモード時のサービス拒否(DoS)の脆弱性(CVE-2022-29859)

三菱電機製の家電製品には、アクセスポイントモード時の DHCP 処理における、Realtek 社製通信チップの脆弱性(CVE-2022-29859)に起因する、解放済みメモリの使用(CWE-416)によるサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威

(1) 悪意のあるスクリプトを含んだメッセージを応答する脆弱性(CVE-2022-33322)

ユーザが不正な Web サイトにアクセスしてしまったり、メールに記載されている不正な URL をクリックしてしまうこと等により、攻撃者は、悪意のあるスクリプトを含んだメッセージを当該製品に送らせ、ユーザのブラウザ上で悪意のあるスクリプトを実行し、ブラウザ内の情報の漏えい等が発生させることができます。なお、本脆弱性により当該製品からの機器データの情報漏えいや、機器の不正操作の影響を受けません。

(2) アクセスポイントモード時のサービス拒否(DoS)の脆弱性(CVE-2022-29859)

アクセスポイントモードで動作中の当該製品の Wi-Fi 通信は、Wi-Fi の受信圏内にいる悪意のある攻撃者によって特別に細工されたデータを受信すると、一時的にサービス停止(DoS)状態に陥り、アクセスポイントモードでの通信ができなくなる可能性があります。結果として、機器登録ができなくなる可能性があります。なお、DoS 状態に陥った場合は、当該製品を手動で再起動するか、又は 10 分経過後に自動的に通常モードに切り替わることにより、復旧いたします。復旧した後は再度、機器登録を行うことができます。

¹ <https://cwe.mitre.org/data/definitions/79.html>

² <https://cwe.mitre.org/data/definitions/416.html>

³ <https://www.ipa.go.jp/security/vuln/CVSSv3.html>

■影響を受ける製品、対策方法及び軽減策・回避策

[1][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 ~ 35.00 です	<p><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、結果として当該製品がサービス拒否(DoS)状態に陥ったり、当該製品が悪意のあるスクリプトを含んだメッセージを応答することにより、ブラウザ上で悪意のあるスクリプトが実行され、ブラウザ内の情報の漏えい等が発生する可能性があります。</p> <p><対策> 無線 LAN ソフトウェア Ver36.00 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。</p> <p>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</p> <p>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、霧ヶ峰 REMOTE 取扱説明書をご参照のうえ霧ヶ峰 REMOTE アプリをインストールして、霧ヶ峰 REMOTE を使用できるように設定ください。</p> <p>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。</p> <p><軽減策・回避策> 無線 LAN ルーターの設定について、以下をご確認ください。</p> <ul style="list-style-type: none"> ・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。 <p>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。</p> <ul style="list-style-type: none"> ・無線 LAN ルーターは外部の人が触れない場所に設置してください。また、フリーWi-Fiとして提供するなど、不特定の第三者にネットワークを開放しないでください。 ・当該製品の URL(IP アドレスやホスト名)を第三者に知られないようにしてください。 <p>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。</p> <ul style="list-style-type: none"> ・OS、ソフトウェア、ウイ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]【冷蔵庫】

型番	対策及び軽減策・回避策
<p>MR-MXD50/57G MR-WXD52/60/70G MR-WZ55/61H MR-MZ54/60H</p> <p>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</p>	<p><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、結果として当該製品がサービス拒否(DoS)状態に陥ったり、当該製品が悪意のあるスクリプトを含んだメッセージを応答することにより、ブラウザ上で悪意のあるスクリプトが実行され、ブラウザ内の情報の漏えい等が発生する可能性があります。</p> <p><対策> 無線 LAN ソフトウェアバージョン Ver01.01 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。</p> <p>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</p> <p><軽減策・回避策> 無線 LAN ルーターの設定について、以下をご確認ください。</p> <ul style="list-style-type: none"> ・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。 ・無線 LAN ルーターは外部の人が触れない場所に設置してください。また、フリーWi-Fiとして提供するなど、不特定の第三者にネットワークを開放しないでください。 ・当該製品の URL(IP アドレスやホスト名)を第三者に知られないようにしてください。 <p>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。</p> <ul style="list-style-type: none"> ・OS、ソフトウェア、ウイ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]【ヒートポンプ給湯機・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
<p>GT-HEM4 GT-RA1 GT-RA2 GT-HR1 RMCB-H6SE-T RMCB-F6SE-T RMCB-D6SE-T</p> <p>影響を受ける製品は上記製品(RMCBから始まる型名の製品に関しては、付属の無線 LAN アダプター)のソフトウェアバージョン 00.83 以前です</p>	<p><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、結果として当該製品がサービス拒否(DoS)状態に陥ったり、当該製品が悪意のあるスクリプトを含んだメッセージを応答することにより、ブラウザ上で悪意のあるスクリプトが実行され、ブラウザ内の情報の漏えい等が発生する可能性があります。</p> <p><対策> 無線 LAN アダプターソフトウェアバージョン Ver00.98 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。</p> <p>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</p> <p>HEMS ご使用の場合は、アップデート非対応です。 GT-HEM4 をご使用の場合、または GT-HR1、RMCB-H6SE-T、RMCB-F6SE-T、RMCB-D6SE-T を HEMS でご使用の場合、以下の軽減策・回避策を実施ください。</p> <p><軽減策・回避策> 無線 LAN 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。 ・無線 LAN ルーターは外部の人が触れない場所に設置してください。また、フリーWi-Fi として提供するなど、不特定の第三者にネットワークを開放しないでください。 ・当該製品の URL(IP アドレスやホスト名)を第三者に知られないようにしてください。</p> <p>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、ウイ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</p>

●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][バス乾燥・暖房・換気システム]

型番	対策及び軽減策・回避策
<p>V-241BZ-RC V-241BZ5-RC WD-240DK-RC WD-240DK2-RC</p> <p>影響を受ける製品は上記製品のバージョン00.65以前です</p>	<p><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、結果として当該製品がサービス拒否(DoS)状態に陥ったり、当該製品が悪意のあるスクリプトを含んだメッセージを応答することにより、ブラウザ上で悪意のあるスクリプトが実行され、ブラウザ内の情報の漏えい等が発生する可能性があります。</p> <p><対策> 無線 LAN アダプターのソフトウェアバージョン Ver00.95 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。</p> <p>[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</p> <p>[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</p> <p><軽減策・回避策> 無線 LAN ルーターの設定について、以下をご確認ください。</p> <ul style="list-style-type: none"> ・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。 <p>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。</p> <ul style="list-style-type: none"> ・無線 LAN ルーターは外部の人が触れない場所に設置してください。また、フリーWi-Fiとして提供するなど、不特定の第三者にネットワークを開放しないでください。 ・当該製品の URL(IP アドレスやホスト名)を第三者に知られないようにしてください。 <p>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。</p> <ul style="list-style-type: none"> ・OS、ソフトウェア、ウイ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]【炊飯器】

型番	対策及び軽減策・回避策
<p>NJ-AWBX10</p> <p>影響を受ける製品は上記製品のバージョン00.75以前です</p>	<p><想定される影響></p> <p>悪意のある攻撃者に脆弱性を悪用された場合、結果として当該製品がサービス拒否(DoS)状態に陥ったり、当該製品が悪意のあるスクリプトを含んだメッセージを応答することにより、ブラウザ上で悪意のあるスクリプトが実行され、ブラウザ内の情報の漏えい等が発生する可能性があります。</p> <p><対策></p> <p>無線 LAN ソフトウェアバージョン Ver00.97 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。</p> <p>[MyMU をご使用の方]</p> <p>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</p> <p>[WiFi らく楽炊飯をご使用の方]</p> <p>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ェアバージョン」から行ってください。</p> <p><軽減策・回避策></p> <p>無線 LAN ルーターの設定について、以下をご確認ください。</p> <ul style="list-style-type: none"> ・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。 ・無線 LAN ルーターは外部の人が触れない場所に設置してください。また、フリーWi-Fi として提供するなど、不特定の第三者にネットワークを開放しないでください。 ・当該製品の URL(IP アドレスやホスト名)を第三者に知られないようにしてください。 <p>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。</p> <ul style="list-style-type: none"> ・OS、ソフトウェア、ウイ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]【三菱 HEMS 用 制御アダプター、無線 LAN アダプター】

型番	対策及び軽減策・回避策
<p>P-HM04WA P-WA01</p> <p>影響を受ける製品は上記製品のバージョン 00.67 以前です</p>	<p><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、結果として当該製品がサービス拒否(DoS)状態に陥ったり、当該製品が悪意のあるスクリプトを含んだメッセージを応答することにより、ブラウザ上で悪意のあるスクリプトが実行され、ブラウザ内の情報の漏えい等が発生する可能性があります。</p> <p><対策> アダプターソフトウェアバージョン Ver00.96 以降で対策しております。 バージョン Ver00.67 以前をご使用の場合には、軽減策・回避策を実施されることを推奨いたします。</p> <p><軽減策・回避策> 無線 LAN ルーターの設定について、以下をご確認ください。</p> <ul style="list-style-type: none"> ・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。 <p>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。</p> <ul style="list-style-type: none"> ・無線 LAN ルーターは外部の人が触れない場所に設置してください。また、フリー Wi-Fi として提供するなど、不特定の第三者にネットワークを開放しないでください。 ・当該製品の URL(IP アドレスやホスト名)を第三者に知られないようにしてください。 <p>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。</p> <ul style="list-style-type: none"> ・OS、ソフトウェア、ウイ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]【ロスナイセントラル換気システム】

型番	対策及び軽減策・回避策
<p>VL-200ZMHSV3-RC</p> <p>影響を受ける製品は上記製品のバージョン 00.71 以前です</p>	<p><想定される影響></p> <p>悪意のある攻撃者に脆弱性を悪用された場合、結果として当該製品がサービス拒否(DoS)状態に陥ったり、当該製品が悪意のあるスクリプトを含んだメッセージを応答することにより、ブラウザ上で悪意のあるスクリプトが実行され、ブラウザ内の情報の漏えい等が発生する可能性があります。</p> <p><対策></p> <p>無線 LAN ソフトウェアバージョン Ver00.94 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。</p> <p>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</p> <p><軽減策・回避策></p> <p>無線 LAN ルーターの設定について、以下をご確認ください。</p> <ul style="list-style-type: none"> ・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。 ・無線 LAN ルーターは外部の人が触れない場所に設置してください。また、フリーWi-Fi として提供するなど、不特定の第三者にネットワークを開放しないでください。 ・当該製品の URL(IP アドレスやホスト名)を第三者に知られないようにしてください。 <p>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。</p> <ul style="list-style-type: none"> ・OS、ソフトウェア、ウイ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]【換気扇用・ロスナイ用スマートスイッチ】

型番	対策及び軽減策・回避策
<p>P-1600SWRC P-04SWRC P-10SWRC</p> <p>影響を受ける製品は上記製品のバージョン 00.90 以前です</p>	<p><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、結果として当該製品がサービス拒否(DoS)状態に陥ったり、当該製品が悪意のあるスクリプトを含んだメッセージを応答することにより、ブラウザ上で悪意のあるスクリプトが実行され、ブラウザ内の情報の漏えい等が発生する可能性があります。</p> <p><対策> ソフトウェアバージョン Ver00.91 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。</p> <p>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</p> <p><軽減策・回避策> 無線 LAN ルーターの設定について、以下をご確認ください。</p> <ul style="list-style-type: none"> 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。 <p>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。</p> <ul style="list-style-type: none"> 無線 LAN ルーターは外部の人が触れない場所に設置してください。また、フリーWi-Fiとして提供するなど、不特定の第三者にネットワークを開放しないでください。 当該製品の URL(IP アドレスやホスト名)を第三者に知られないようにしてください。 <p>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。</p> <ul style="list-style-type: none"> OS、ソフトウェア、ウイ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)

■更新履歴

2023 年 10 月 26 日

- 「影響を受ける製品、対策方法及び軽減策・回避策」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
[6]【三菱 HEMS 用 制御アダプター、無線 LAN アダプター】

2023 年 2 月 21 日

- 「概要」、「脆弱性の説明」及び「脆弱性がもたらす脅威」を補足。
- 「影響を受ける製品、対策方法及び軽減策・回避策」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
[2]【冷蔵庫】
[3]【ヒートポンプ給湯機・HEMS 対応アダプター、無線 LAN アダプター】
[4]【バス乾燥・暖房・換気システム】
[5]【炊飯器】
[7]【ロスナイセントラル換気システム】