複数の当社家電製品のアクセスポイントモード時の Wi-Fi 接続処理における Realtek 社製チップに起因するサービス拒否(DoS)の脆弱性

公開日 2022 年 11 月 15 日
最終更新日 2023 年 10 月 26 日
三菱電機株式会社

■概要

三菱電機製の家電製品に、アクセスポイントモード時の Wi-Fi 接続処理において、Realtek 社製チップの脆弱性(CVE-2022-34326)に起因する、デッドロック(CWE-833)[1]によるサービス拒否(DoS)の脆弱性が存在することが判明しました。アクセスポイントモードは、機器登録の際に、当社製品を外部接続機器(無線 LAN ルーター)に接続するために使用するモードです。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、アクセスポイントモードで動作中の当該製品の Wi-Fi 通信が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。本脆弱性の影響を受ける製品名を「■影響を受ける製品、対策方法及び軽減策・回避策」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完了して通常使用されている場合

■CVSS スコア [2]

CVE-2022-34326 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

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 Wi-Fi 接続処理において、デッドロック(CWE-833)に起因する、サービス拒否(DoS)の脆弱性が存在します(CVE-2022-34326)。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。

■脆弱性がもたらす脅威

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、アクセスポイントモードで動作中の当該製品の Wi-Fi 通信が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/833.html

2 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-FD4023S MSZ-FD5623S MSZ-FD6323S MSZ-FD7123S MSZ-FD8023S MSZ-HXV2523 MSZ-HXV2823S MSZ-HXV4023S MSZ-HXV5623S MSZ-HXV6323S MSZ-HXV7123S MSZ-HXV8023S MSZ-VXV4023S MSZ-VXV5623S MSZ-VXV6323S MSZ-VXV7123S MSZ-VXV8023S MSZ-ZD2523 MSZ-ZD2823S MSZ-ZD4023S MSZ-ZD5623S MSZ-ZD6323S MSZ-ZD7123S MSZ-ZD8023S MSZ-FZ4022S MSZ-FZ5622S MSZ-FZ6322S MSZ-FZ7122S MSZ-FZ8022S MSZ-FZ9022S MSZ-ZW2222 MSZ-ZW2522 MSZ-ZW2822 MSZ-ZW2822S MSZ-ZW3622 MSZ-ZW3622S MSZ-ZW4022S MSZ-ZW5622S MSZ-ZW6222S MSZ-ZW7122S MSZ-ZW8022S MSZ-ZW9022S MSZ-FZV4022S MSZ-FZV5622S MSZ-FZV6322S MSZ-FZV7122S MSZ-FZV8022S MSZ-FZV9022S MSZ-ZXV2222 MSZ-ZXV2522 MSZ-ZXV2822 MSZ-ZXV2822S MSZ-ZXV3622 MSZ-ZXV3622S MSZ-ZXV4022S MSZ-ZXV5622S MSZ-ZXV6222S MSZ-ZXV7122S MSZ-ZXV8022S MSZ-ZXV9022S MSZ-EM2222E1	<想定される影響> アクセスポイントモードによる Wi-Fi 接続処理において、悪意のある攻撃者によって細工されたデータを受信すると、当該製品の Wi-Fi 通信が一時的にサービス停止(DoS)状態に陥る可能性があります。結果として、DoS 状態の間は Wi-Fi 接続作業ができません。 ＜対策＞ 無線 LAN ソフトウェア Ver37.00 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＞ 当該製品のアクセスポイントモードの SSID 及び KEY を不特定の第三者に知られないようにしてください。 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。

MSZ-EM2522E1	
MSZ-EM2822E1	
MSZ-EM3622E1	
MSZ-EM4022E1S	
MSZ-EM5622E1S	
MSZ-EM6322E1S	
MSZ-EM7122E1S	
MSZ-EM8022E1S	
MSZ-EM9022E1S	
MSZ-FD4022S	
MSZ-FD5622S	
MSZ-FD6322S	
MSZ-FD7122S	
MSZ-FD8022S	
MSZ-HXV2522	
MSZ-HXV2822S	
MSZ-HXV4022S	
MSZ-HXV5622S	
MSZ-HXV6322S	
MSZ-HXV7122S	
MSZ-HXV8022S	
MSZ-VXV4022S	
MSZ-VXV5622S	
MSZ-VXV6322S	
MSZ-VXV7122S	
MSZ-VXV8022S	
MSZ-ZD2522	
MSZ-ZD2822S	
MSZ-ZD4022S	
MSZ-ZD5622S	
MSZ-ZD6322S	
MSZ-ZD7122S	
MSZ-ZD8022S	
MSZ-FZ4021S	
MSZ-FZ5621S	
MSZ-FZ6321S	
MSZ-FZ7121S	
MSZ-FZ8021S	
MSZ-FZ9021S	
MSZ-ZW2221	
MSZ-ZW2521	
MSZ-ZW2821	
MSZ-ZW2821S	
MSZ-ZW3621	
MSZ-ZW3621S	
MSZ-ZW4021S	
MSZ-ZW5621S	
MSZ-ZW6321S	
MSZ-ZW7121S	
MSZ-ZW8021S	
MSZ-ZW9021S	
MSZ-FZV4021S	
MSZ-FZV5621S	
MSZ-FZV6321S	
MSZ-FZV7121S	
MSZ-FZV8021S	
MSZ-FZV9021S	
MSZ-ZXV2221	
MSZ-ZXV2521	
MSZ-ZXV2821	
MSZ-ZXV2821S	
MSZ-ZXV3621	
MSZ-ZXV3621S	
MSZ-ZXV4021S	
MSZ-ZXV5621S	

MSZ-ZXV6321S MSZ-ZXV7121S MSZ-ZXV8021S MSZ-ZXV9021S MSZ-EM2221E9 MSZ-EM2521E9 MSZ-EM2821E9 MSZ-EM3621E9 MSZ-EM4021E9S MSZ-EM5621E9S MSZ-EM6321E9S MSZ-EM7121E9S MSZ-EM8021E9S MSZ-EM9021E9S MSZ-FZ4020S MSZ-FZ5620S MSZ-FZ6320S MSZ-FZ7120S MSZ-FZ8020S MSZ-FZ9020S MSZ-ZW2220 MSZ-ZW2520 MSZ-ZW2820 MSZ-ZW2820S MSZ-ZW3620 MSZ-ZW3620S MSZ-ZW4020S MSZ-ZW5620S MSZ-ZW6320S MSZ-ZW7120S MSZ-ZW8020S MSZ-ZW9020S MSZ-FZV4020S MSZ-FZV5620S MSZ-FZV6320S MSZ-FZV7120S MSZ-FZV8020S MSZ-FZV9020S MSZ-ZXV2220 MSZ-ZXV2520 MSZ-ZXV2820 MSZ-ZXV2820S MSZ-ZXV3620 MSZ-ZXV3620S MSZ-ZXV4020S MSZ-ZXV5620S MSZ-ZXV6320S MSZ-ZXV7120S MSZ-ZXV8020S MSZ-ZXV9020S MSZ-EM2220E8 MSZ-EM2520E8 MSZ-EM2820E8 MSZ-EM3620E8 MSZ-EM4020E8S MSZ-EM5620E8S MSZ-EM6320E8S MSZ-EM7120E8S MSZ-EM8020E8S MSZ-EM9020E8S 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 30.00～36.00 です	

●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
MR-MXD50G MR-MXD57G MR-WXD52G MR-WXD60G MR-WXD70G MR-WZ55H MR-WZ61H MR-MZ54H MR-MZ60H 影響を受ける製品は上記製品のバージョン 00.43 と 00.68 です	〈想定される影響〉 アクセスポイントモードによる Wi-Fi 接続処理において、悪意のある攻撃者によって細工されたデータを受信すると、当該製品の Wi-Fi 通信が一時的にサービス停止(DoS)状態に陥る可能性があります。結果として、DoS 状態の間は Wi-Fi 接続作業ができません。 ＜対策＞ 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。 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＞ 当該製品のアクセスポイントモードの SSID 及び KEY を不特定の第三者に知られないようにしてください。 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]【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
GT-HEM4 GT-RA1 GT-RA2 GT-HR1 RMCB-H6SE-T RMCB-F6SE-T RMCB-D6SE-T 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おいては、付属の無線 LAN アダプター)のソフトウェアバージョン 01.00 以前です	〈想定される影響〉 アクセスポイントモードによる Wi-Fi 接続処理において、悪意のある攻撃者によって細工されたデータを受信すると、当該製品の Wi-Fi 通信が一時的にサービス停止(DoS)状態に陥る可能性があります。結果として、DoS 状態の間は Wi-Fi 接続作業ができません。 ＜対策＞ 無線 LAN アダプターソフトウェアバージョン Ver01.16 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 HEMS ご使用の場合には、アップデートに非対応です。 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。 ＜軽減策・回避策＞ 当該製品のアクセスポイントモードの SSID 及び KEY を不特定の第三者に知られないようにしてください。 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]【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 V-241BZ5-RC WD-240DK-RC WD-240DK2-RC 影響を受ける製品は上記製品のバージョン00.95以前です	<想定される影響> アクセスポイントモードによる Wi-Fi 接続処理において、悪意のある攻撃者によって細工されたデータを受信すると、当該製品の Wi-Fi 通信が一時的にサービス停止(DoS)状態に陥る可能性があります。結果として、DoS 状態の間は Wi-Fi 接続作業ができません。 ＜対策＞ 無線 LAN アダプターのソフトウェアバージョン Ver01.13 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＞ 当該製品のアクセスポイントモードの SSID 及び KEY を不特定の第三者に知られないようにしてください。 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　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-HM04WA P-WA01 影響を受ける製品は上記製品のバージョン00.96以前です	<想定される影響> アクセスポイントモードによる Wi-Fi 接続処理において、悪意のある攻撃者によって細工されたデータを受信すると、当該製品の Wi-Fi 通信が一時的にサービス停止(DoS)状態に陥る可能性があります。結果として、DoS 状態の間は Wi-Fi 接続作業ができません。 ＜対策＞ アダプターソフトウェアバージョン Ver01.14 以降で対策しております。 バージョン Ver00.96 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。 ＜軽減策・回避策＞ 当該製品のアクセスポイントモードの SSID 及び KEY を不特定の第三者に知られないようにしてください。 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]【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
VL-200ZMHSV3-RC 影響を受ける製品は上記製品のバージョン 00.94 以前です	<想定される影響> アクセスポイントモードによる Wi-Fi 接続処理において、悪意のある攻撃者によって細工されたデータを受信すると、当該製品の Wi-Fi 通信が一時的にサービス停止(DoS)状態に陥る可能性があります。結果として、DoS 状態の間は Wi-Fi 接続作業ができません。 ＜対策＞ 無線 LAN ソフトウェアバージョン Ver01.12 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＞ 当該製品のアクセスポイントモードの SSID 及び KEY を不特定の第三者に知られないようにしてください。 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]【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-1600SWRC P-04SWRC P-10SWRC 影響を受ける製品は上記製品のバージョン 00.92 以前です	<想定される影響> アクセスポイントモードによる Wi-Fi 接続処理において、悪意のある攻撃者によって細工されたデータを受信すると、当該製品の Wi-Fi 通信が一時的にサービス停止(DoS)状態に陥る可能性があります。結果として、DoS 状態の間は Wi-Fi 接続作業ができません。 ＜対策＞ ソフトウェアバージョン Ver01.10 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＞ 当該製品のアクセスポイントモードの SSID 及び KEY を不特定の第三者に知られないようにしてください。 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）

■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
[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]【三菱 HEMS 用　制御アダプター、無線 LAN アダプター】
[6]【ロスナイセントラル換気システム】
[7]【換気扇用・ロスナイ用スマートスイッチ】
・「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「型番」を修正

[1]【ルームエアコン・無線 LAN アダプター】 MSZ-FZ5622S