Amazon FreeRTOS のメモリ割り当て処理におけるサービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性

公開日 2021 年 9 月 2 日
最終更新日 2021 年 11 月 30 日
三菱電機株式会社

■概要

Amazon FreeRTOS のメモリ割り当て処理に対して、メモリサイズの検証の不備により、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性(CVE-2021-31571)が公開されました。本脆弱性は、BadAllock と呼ばれている一連の脆弱性の内の一つです。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、サービス拒否(DoS)状態に陥らされたり、悪意のあるプログラムを実行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-2021-31571: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H 基本値:7.7

■脆弱性の説明

メモリ割り当て処理では、リクエストされるメモリサイズが一定の範囲に収まっていることや計算処理が正しく行われることを検証する必要がありますが、これらの検証の不備により、Amazon FreeRTOS のメモリ割り当て処理に対して、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性(CVE-2021-31571)が公開されました。当社製品も本脆弱性の影響を受ける可能性があります。(CWE-190)

■脆弱性がもたらす脅威

攻撃者は、特別に細工したデータをアプリケーションへ渡し、整数オーバーフローを発生させることにより、対象機器をサービス拒否(DoS)状態に陥らせたり、悪意のあるプログラムを実行することができます。

■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 30.00～33.00 です	〈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、サービス拒否(DoS)状態に陥ったり、悪意のあるプログラムが実行され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)

[2]【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	<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、サービス拒否(DoS)状態に陥ったり、悪意のあるプログラムが実行され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）

[3]【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	<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、サービス拒否(DoS)状態に陥ったり、悪意のあるプログラムが実行され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）

[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 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	<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、サービス拒否(DoS)状態に陥ったり、悪意のあるプログラムが実行され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）

[5]【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	<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、サービス拒否(DoS)状態に陥ったり、悪意のあるプログラムが実行され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）

[6]【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	<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、サービス拒否(DoS)状態に陥ったり、悪意のあるプログラムが実行され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）

■更新履歴
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
[1]【ルームエアコン・無線 LAN アダプター】 PAC-SK43ML
[2]【冷蔵庫】 MR-MXD50/57G、MR-WXD52/60/70G
[3]【HEMS 対応アダプター、無線 LAN アダプター】 GT-HEM4、GT-RA1、GT-RA2
[4]【バス乾燥・暖房・換気システム】 V-241BZ-RC、WD-240DK-RC
[5]【炊飯器】 NJ-AWBX10
[6]【三菱 HEMS 用　制御アダプター】 P-HM04WA