TCP/IP スタックにおける複数の脆弱性(Ripple20)の影響について

公開日 2020 年 9 月 24 日
最終更新日 2020 年 10 月 29 日
三菱電機株式会社

■概要

TCP/IP スタックにおける 19 件の脆弱性(通称 Ripple20)が公開されました。これらの脆弱性を悪意のある攻撃者に悪用された場合、情報の漏えい、情報の破壊・改ざん、サービスの停止(DoS)、悪意のあるプログラムの実行等、様々な影響を受ける恐れがあります。複数の当社製品において、これらの脆弱性の一部の影響を受ける可能性があることが判明しました。

現時点で判明している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。本脆弱性の影響を受ける製品名、対策及び軽減策・回避策を順次更新いたします。

■脆弱性の説明

Treck 社製 IP スタック及び図研エルミック社製 IP スタック(KASAGO®)には、下記 19 件の脆弱性が存在します。当社製品もこれらの脆弱性の一部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(1～19)を掲載しますので、ご確認ください。**

1. IPv4/UDP コンポーネントにリモートから悪意のあるプログラムが実行される脆弱性(CVE-2020-11896)
2. IPv6 コンポーネントにリモートから悪意のあるプログラムが実行される脆弱性(CVE-2020-11897)
3. IPv4/ICMPv4 コンポーネントに情報漏えいの脆弱性(CVE-2020-11898)
4. IPv6 コンポーネントに情報漏えい及びサービス拒否(DoS)の脆弱性(CVE-2020-11899)
5. IPv4 トンネリングコンポーネントにサービス拒否(DoS)の脆弱性(CVE-2020-11900)
6. DNS リゾルバコンポーネントにリモートから悪意のあるプログラムが実行される脆弱性(CVE-2020-11901)
7. IPv6 over IPv4 トンネリングコンポーネントに情報漏えいの脆弱性(CVE-2020-11902)
8. DHCP コンポーネントに情報漏えいの脆弱性(CVE-2020-11903)
9. メモリ割り当てコンポーネントに情報破壊、サービス拒否(DoS)及びリモートから悪意のあるプログラムが実行される脆弱性(CVE-2020-11904)
10. DHCPv6 コンポーネントに情報漏えいの脆弱性(CVE-2020-11905)
11. イーサネットリンクレイヤコンポーネントにサービス拒否(DoS)の脆弱性(CVE-2020-11906)
12. TCP コンポーネントにサービス拒否(DoS)の脆弱性(CVE-2020-11907)
13. DHCP コンポーネントに情報漏えいの脆弱性(CVE-2020-11908)
14. IPv4 コンポーネントにサービス拒否(DoS)の脆弱性(CVE-2020-11909)
15. ICMPv4 コンポーネントに情報漏えいの脆弱性(CVE-2020-11910)
16. ICMPv4 コンポーネントにサービス拒否(DoS)の脆弱性(CVE-2020-11911)
17. TCP コンポーネントに情報漏えいの脆弱性(CVE-2020-11912)
18. IPv6 コンポーネントに情報漏えいの脆弱性(CVE-2020-11913)
19. ARP コンポーネントに情報漏えいの脆弱性(CVE-2020-11914)

■脆弱性がもたらす脅威

製品毎に想定される脅威は異なりますが、悪意のある攻撃者に脆弱性を悪用された場合に、情報の漏えい、情報の破壊・改ざん、サービスの停止(DoS)、悪意のあるプログラムの実行等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

[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 （3、6、9、12、13、16、17、19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、サービスの停止(DoS)、情報の漏えい、情報の改ざん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＞ ・インターネットに接続する場合、計測ユニットは据付工事説明書に従い、製品に同梱の情報収集ユニットに接続してご使用下さい。エコガイドでは、悪意のある攻撃者に対して、情報収集ユニットが本脆弱性の影響を軽減します。 情報収集ユニットより上流のルーターなどの機器については、下段共通項目をご参照ください。
PV-DR006L-IFU-MRC-M （3、6、9、12、13、16、17、19の影響を受ける可能性があります）	〈想定される影響〉 本製品はインターネット経由の攻撃の影響を受けることはありません。 ＜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＞ ・本製品はインターネット経由の攻撃の影響を受けることはありません。ただし、当社指定の情報収集ユニットを追加購入してインターネットに接続する場合は、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。エコガイドでは、悪意のある攻撃者に対して、情報収集ユニットが本脆弱性の影響を軽減します。（当社指定以外の HEMS ユニット、市販のルーターなどには直接接続をしないでください。） 情報収集ユニットより上流のルーターなどの機器については、下段共通項目をご参照ください。
上記 3 機種の共通項目	＜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接続しているルーターが有線の場合は以下をご確認ください。 ・有線 LAN 用ルーターの設定を変更されている場合、インターネットからの不正アクセスを困難とし、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。 有線 LAN の設定についてはルーターメーカーにお問い合わせください。 ■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 の設定についてはルーターメーカーにお問い合わせください。 ■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。 ・ウィルス対策ソフト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)

ﾌﾘｰﾀﾞｲﾔﾙ,ﾅﾋﾞﾀﾞ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
GT-HEM1 GT-HEM2 GT-HEM3 GT-HEM3-M 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 MAC-884IF MAC-888IF P-01HMA P-HM02WA P-HM03WA VEZ-HM01WA （3、6、9、12、13、16、17、19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、サービスの停止(DoS)、情報の漏えい、情報の改ざん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が以下であるかご確認ください。 ・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 の設定についてはルーター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。 ・ウィルス対策ソフト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)
ﾌﾘｰﾀﾞｲﾔﾙ,ﾅﾋﾞﾀﾞ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) （3、6、9、12、13、16、17、19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、サービスの停止(DoS)、情報の漏えい、情報の改ざん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 の設定についてはルーター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。 ・ウィルス対策ソフト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)
ﾌﾘｰﾀﾞｲﾔﾙ,ﾅﾋﾞﾀﾞ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 （3、6、9、12、13、16、17、19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、サービスの停止(DoS)、情報の漏えい、情報の改ざん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 の設定についてはルーター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。 ・ウィルス対策ソフト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)
ﾌﾘｰﾀﾞｲﾔﾙ,ﾅﾋﾞﾀﾞｲﾔﾙをご利用いただけない場合　03-3414-9655(有料)

[5]【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 （3、6、9、12、13、16、17、19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、サービスの停止(DoS)、情報の漏えい、情報の改ざん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 に無線 LAN 接続してください。 無線ルーターの設定が以下であるかご確認ください。 ・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 の設定についてはルーター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。 ・ウィルス対策ソフト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)
ﾌﾘｰﾀﾞｲﾔﾙ,ﾅﾋﾞﾀﾞｲﾔﾙをご利用いただけない場合　03-3414-9655(有料)

[6]【ネットワークカメラ】

型番	対策及び軽減策・回避策
NC-6000 NC-6000B21 NC-6000B22 NC-6100 NC-6100B21 NC-6100B22 NC-6400 NC-6500 NC-6600 NC-6700 NC-8000 NC-8000A NC-8000B21 NC-8000B22 NC-8600 NC-8600A NC-8800 NC-8800A NC-8800AS （11、12、15、16、17、19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、サービスの停止(DoS)の影響を受ける可能性があります。 ＜対策＞ 本脆弱性に対応したソフトウェアを準備しております。 以下の手順でネットワークカメラの利用状態を確認し、対応ソフトウェアの適用が必要かをご検討ください。 1. ネットワークカメラを接続しているネットワークが、インターネットと外部接続されているかどうかを確認ください。接続されていない場合は、対策は不要です。 2. インターネットと外部接続されている場合は、ファイアウォールやルーターにて、インターネットからの不正アクセスを困難とし、インターネット上での存在が特定されないような設定となっていることを確認ください。このような設定となっていない場合は適切な設定に変更ください。 ファイアウォールやルーターの設定については各メーカーにお問い合わせください。 3. 何らかの理由で「2」に示す設定が困難な場合は、保守終了品を除き、本脆弱性に対応したソフトウェアを提供しますので、ご購入いただいた支社、代理店にご相談ください。

●お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、代理店にご相談ください。

■上記製品以外に対するお客様からのお問い合わせ先
https://www.mitsubishielectric.co.jp/contact/ssl/php/1333/kiyaku.php?fid=1333&Vul=Ripple20

■参考情報
●Japan Vulnerability Notes「JVNVU#94736763　Treck 製 IP スタックに複数の脆弱性」
https://jvn.jp/vu/JVNVU94736763/index.html
●CERT/CC Vulnerability Note “VU#257161 Treck IP stacks contain multiple vulnerabilities”
https://www.kb.cert.org/vuls/id/257161
●ICS Advisory “ICSA-20-168-01 Treck TCP/IP Stack”
https://www.us-cert.gov/ics/advisories/icsa-20-168-01
●JSOF “Ripple20”
https://www.jsof-tech.com/ripple20/
●Treck Inc. “Vulnerability Response Information”
https://treck.com/vulnerability-response-information/
●図研エルミック株式会社「KASAGO 製品における脆弱性に関するお知らせ」
https://www.elwsc.co.jp/news/4136/

■更新履歴
2020 年 10 月 29 日
影響を受ける製品を追加（[6]）