2020 年 6 月 17 日

お客様各位

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

平素より、弊社製品をご利用頂き誠に有難う御座います。
この度、弊社 KASAGO 製品において以下の脆弱性が存在することが判明致しました。
対象のお客様におかれましては、多大なるご迷惑をお掛け致します事、深くお詫び申し上げます。

この脆弱性が悪用された場合、悪意ある第三者の攻撃により意図しない動作をする危険性が御座います。本脆弱性の詳細につきましては、下記をご参照頂き回避策の実施又は、弊社が提供するパッチプログラムの適用をお願い申し上げます。

本件に関するお問い合わせ先

担当営業又は下記問い合わせ窓口までお問合せ下さい。

TEL：045-624-8002　E-Mail：kasago_vulnerability@elwsc.co.jp

1. 影響を受ける製品

- KASAGO IPv4 Light
- KASAGO IPv4
- KASAGO IPv6/v4 Dual
- KASAGO DHCPv6

脆弱性に影響を受ける製品に〇を記載しております。

()内には製品に含まれる該当プロトコルを記載しております。

該当製品/Version CVE番号	KASAGO IPv4 Light	KASAGO IPv4	KASAGO IPv6(Dual)	KASAGO DHCPv6	該当バージョン
CVE-2019-12264		〇 (DHCP/Bootp Client)	〇 (DHCP/Bootp Client)		Ver6.0.1.33以前のバージョン
CVE-2020-11896			〇 (IP)		Ver6.0.1.33以前のバージョン
CVE-2020-11897			〇 (IPv6)		Ver4.7.1.26以前のバージョン
CVE-2020-11898			〇 (IP)		Ver6.0.1.33以前のバージョン
CVE-2020-11899			〇 (IPv6)		Ver6.0.1.33以前のバージョン
CVE-2020-11900			〇 (IP)		Ver6.0.1.33以前のバージョン
CVE-2020-11901		〇 (DNS Resolver)	〇 (DNS Resolver)		Ver6.0.1.33以前のバージョン
CVE-2020-11902			〇 (ICMP)		Ver6.0.1.33以前のバージョン
CVE-2020-11903		〇 (DHCP Client)	〇 (DHCP Client)		Ver6.0.1.33以前のバージョン
CVE-2020-11904	〇 (全般)	〇 (全般)	〇 (全般)		Ver6.0.1.33以前のバージョン
CVE-2020-11905				〇	Ver6.0.1.33以前のバージョン
CVE-2020-11906	〇 (Ether)	〇 (Ether)	〇 (Ether)		Ver6.0.1.33以前のバージョン
CVE-2020-11907	〇 (TCP)	〇 (TCP)	〇 (TCP)		Ver6.0.1.33以前のバージョン
CVE-2020-11908		〇 (DHCP/Bootp Client)	〇 (DHCP/Bootp Client)		Ver4.7.1.26以前のバージョン
CVE-2020-11909	〇 (IP)	〇 (IP)	〇 (IP)		Ver6.0.1.33以前のバージョン
CVE-2020-11910	〇 (ICMP)	〇 (ICMP)	〇 (ICMP)		Ver6.0.1.33以前のバージョン
CVE-2020-11911	〇 (ICMP)	〇 (ICMP)	〇 (ICMP)		Ver6.0.1.33以前のバージョン
CVE-2020-11912	〇 (TCP)	〇 (TCP)	〇 (TCP)		Ver6.0.1.33以前のバージョン
CVE-2020-11913			〇 (IPv6)		Ver6.0.1.33以前のバージョン
CVE-2020-11914	〇 (ARP)	〇 (ARP)	〇 (ARP)		Ver6.0.1.33以前のバージョン

2. 脆弱性の概要と回避策

該当する脆弱性に対して、概要、対象、影響、最新バージョン(Ver6.0.1.33)における回避策について説明します。「影響」欄中の「悪意ある通信対象」または「悪意ある xxx」という表現は、故意に Ethernet 規格を外れる通信を行う通信相手の事を意味します。Ethernet 規格で許されている通信内容にて現象が発生する項目では「悪意ある xxx」という表現を致しません。

【CVE-2019-12264】

概要: DHCP サーバから通知された不正な IP アドレスを排除できず、LAN に接続された機器間の通信が不正となる可能性がある。

対象:　KASAGO IPv4 及び KASAGO IPv6 に含まれる DHCP/Bootp クライアント

影響:　悪意ある DHCP サーバからマルチキャストアドレス[1]が KASAGO の DHCP クライアントに対して割り当てられた場合、割り当てられたマルチキャストアドレスを利用して通信を開始する。そのため、LAN に接続された Ethernet 機器の動作が不正となる可能性があります。

補足 1:　本 CVE は他社製 TCP/IP スタックに対する指摘ですが、独自調査の結果 KASAGO にも同様の脆弱性がある事が判明しました。

補足 2:　DHCP クライアント機器側の不正な IP アドレスとして、マルチキャストアドレスおよび“0.0.0.0”、“ブロードキャストアドレス”がありますが、KASGO の DHCP クライアントはマルチキャストアドレスが渡された場合に動作不正となります。
通常、悪意ある DHCP サーバが存在するネットワーク上では正常な通信は期待できないため、KASAGO を利用した機器のみが問題となる状況とはなりません。

回避策:　アプリケーションにて DHCP クライアントが IP アドレス取得時に自 IP アドレスを確認し、不正 IP アドレスの場合通信動作を停止する。

【CVE-2020-11896】

概要:　IPv4 トンネル化され意図的に分割(フラグメント)された IP パケットを正しく処理できず動作停止する可能性がある。

対象:　KASAGO IPv6(Dual)に含まれる IP 処理

影響:　悪意ある通信対象から IPv4 トンネル化され意図的にフラグメントされたパケットを受信すると、受信バッファ外のメモリを破壊し、KASAGO が動作停止する可能性があります。

補足:　本脆弱性はドライバの分割受信が有効になっている場合は発生いたしません。

回避策:　“TM_USE_DRV_SCAT_RECV”を設定する(ドライバの分割受信を有効にする)[2]。

【CVE-2020-11897】

概要:　IPv6 のルーティングヘッダ部分でフレーム分割された Ether フレームを正しく処理できず、意図しないデータが外部に送信される可能性がある。

対象:　Ver. 4.7.1.26 以前の KASAGO IPv6(Dual)に含まれる IPv6 処理

影響:　悪意ある通信相手が送信した IPv6 ルーティングヘッダ内部でフラグメントのあるデータを受信した場合、フラグメントされた後半の IPv6 ルーティングヘッダ情報をアップデート

---

[1] マルチキャストアドレスとはマルチキャストを示す IP アドレスであり、“224.0.0.0～239.255.255.255”の範囲が対象となります。

[2] ドライバ分割受信を有効にする場合(TM_USE_DRV_SCAT_RECV の有効化)でもドライバ部分に修正は必要ありません。

しないままルーティングヘッダ処理を行うため、動作不正となり意図しないデータが外部に送信される可能性があります。

補足: IPv6 の規格は最小の MTU 値が 1280 となっており、通常の機器が本パケットを出力することはありません。
また、RFC5095 にて今回の問題が発生するケース(RH0: ルーティング・ヘッダ・タイプ 0)は廃止となっています。KASAGO 4.7.1.26 より後のバージョンでは RH0 がサポート対象ではなくフレームが破棄されるため、本脆弱性は発生しません。

回避策: TM_6_USE_IP_FORWARD を定義しない(IPv6 転送を有効としない)。
あるいは最新バージョン(Ver6.0.1.33)の利用

【CVE-2020-11898】

概要: IPv4 トンネル化され、不正なデータを持つ分割(フラグメント)された ICMP パケットを受信した場合、正常に処理できず意図しないデータが外部に送信される可能性がある。

対象: KASAGO IPv6(Dual)に含まれる IP 処理
→ IPv6/IPv4 デュアル動作時

影響: 悪意ある通信対象から意図的に以下に記載する条件のすべてに該当する不正な ICMP パケットを受信した場合に ICMP エラー処理でフラグメントされた後方のデータを利用せずに受信したバッファ外のデータでエラー応答するため、意図しないデータが外部へ送信される可能性があります。

- ICMP 処理でエラーを発生させる
- IPv4 トンネルされている
- フラグメントされている

補足: IPv6/IPv4 のデュアル動作のみ本現象に該当します。IPv6 及び IPv4 の単体動作で利用する場合、本現象は発生いたしません。
また、本脆弱性はドライバの分割受信が有効になっている場合は発生いたしません。

回避策: IPv6/IPv4 デュアル動作を利用しない。
または“TM_USE_DRV_SCAT_RECV”を設定する(ドライバの分割受信を有効にする)[3]。

[3] ドライバ分割受信を有効にする場合(TM_USE_DRV_SCAT_RECV の有効化)でもドライバ部分に修正は必要ありません。

【CVE-2020-11899】

概要: アプリケーションからの送信宛先に TCP/IP スタックに保持されているスコープ ID より大きな値が指定された場合に、管理領域外の不正なデータを参照して処理を実行するため、意図しないデータが送信される可能性がある。

対象: KASAGO IPv6(Dual)に含まれる IPv6 処理

影響: アプリケーションがマルチキャスト宛ての UDP 送信を実行時に、宛先アドレス情報に登録されているスコープ ID 値より大きな値を指定した場合、不正なデータを参照して処理を実行するため、内部に保存されている意図しないデータが送信される可能性があります。

回避策: アプリケーションによるスコープ ID の確認を実施し範囲外のスコープ ID に対する送信の抑制

【CVE-2020-11900】

概要: KASAGO が許容する IP トンネル数[4]以上にネストしたパケットを受信した場合、メモリの 2 重解放が発生し、動作停止する可能性がある

対象: KASAGO IPv6(Dual)の IP 処理

影響: KASAGO IPv6 が 4 以上の IP トンネルのネストを持つ IP パケットを受信した場合、カプセル取り出し処理でメモリを 2 重解放しメモリ破壊を発生し動作不正となる可能性があります。

補足: 通常の機器では IP トンネル 2 以上を使うユースケースは無いと考えられます。

回避策: 最新バージョン(Ver6.0.1.33)における回避策は御座いません。
パッチ適用をご検討ください。

【CVE-2020-11901】

概要: 非常に大きい DNS ラベル長を持つパケットを受信した場合、メモリ破壊を発生するため動作停止する可能性がある。

対象: KASAGO IPv4 及び KASAGO IPv6(Dual)内部の DNS リゾルバ処理

影響: KASAGO の DNS リゾルバは DNS 圧縮ラベルを利用し、合計ラベル長が 65535 を超える DNS 応答を受信すると、KASAGO 管理のメモリを破壊し、KASAGO が動作停止する可能性があります。

回避策: 最新バージョン(Ver6.0.1.33)における回避策は御座いません。
パッチ適用をご検討ください。

---

[4] KASAGO は IP トンネルに 3 ネストまで対応します。

【CVE-2020-11902】

概要: 不正な IPv4 ヘッダを持つ ICMP パケットを受信した場合に、内部に保存されている意図しないデータが送信される可能性がある。

対象: KASAGO IPv6 の ICMP 処理

影響: 悪意ある通信相手から IPv6 ヘッダを持たない IPv6 でカプセル化された IPv4 の ICMP パケットを受信した場合、IPv6 ヘッダの確認をせずにヘッダ情報をアクセスすることで内部に保存されている意図しないデータが送信される可能性があります。

補足: IPv6/IPv4 のデュアル動作のみ本現象に該当します。IPv6 及び IPv4 の単体動作で利用する場合、本現象は発生いたしません。

回避策: IPv6/IPv4 デュアル動作を利用しない。

【CVE-2020-11903】

概要: 不正な DHCP 応答受信時、動作停止または内部に保存されている意図しないデータが送信される可能性がある。

対象: KASAGO IPv4 および KASAGO IPv6(Dual)に含まれる DHCP クライアント

影響: 悪意ある通信対象から、KASAGO DHCPc が DHCP リクエストを送信していない状況で不正なオプションを含む DHCP Ack を受信した際、KASAGO が管理する不正なバッファを参照するため、KASAGO が動作停止する可能性があります。また、DHCP Ack の内容がドメイン名の場合、バッファ外のデータをドメイン名として利用してしまう事で内部情報が出力される可能性があります。

回避策: 最新バージョン(Ver6.0.1.33)における回避策は御座いません。
パッチ適用をご検討ください。

【CVE-2020-11904】

概要: バッファ取得関数にて不正なサイズが指定される場合に不正な領域へのポインタを返却するため、動作不正となる可能性がある。

対象: KASAGO IPv4 Lite および KASAGO IPv4、KASAGO IPv6(Dual)の内部関数“tfGetRawBuffer()”を利用するアプリケーション

影響: アプリケーションから“tfGetRawBuffer()”関数のバッファサイズに 0xFFFFFFFD 以上を利用する場合、不正なポインタが返却されるため、アプリケーション動作が不正となる可能性があります。

補足: “tfGetRawBuffer()”は KASAGO の内部関数ですが、KASAGO の処理において該当サイズで本関数を呼び出すことは無いため、KASAGO 単体で動作不正となる事はありません。

回避策: アプリケーションによるバッファサイズ修正

【CVE-2020-11905】

概要: DHCPv6 サーバからの不正な通信を排除できず不正な動作となり、動作停止または内部に保存されている意図しないデータが送信される可能性がある。

対象: KASAGO DHCPv6 クライアントオプション

影響: 悪意のある DHCPv6 サーバからオプションの Length より短いデータを持つパケット受信した場合、受信バッファ外のデータを参照して処理を継続するため動作不正と可能性があります。また、不正オプションがドメイン検索リストの場合、バッファ外のデータをドメイン名として利用してしまう事で内部情報が出力される可能性があります。

回避策: 最新バージョン(Ver6.0.1.33)における回避策は御座いません。
パッチ適用をご検討ください。

【CVE-2020-11906】

概要: Ethernet ヘッダサイズより短い Ethernet フレームを受信した場合、動作停止する可能性がある

対象: KASAGO IPv4 Lite および KASAGO IPv4、KASAGO IPv6(Dual)内の Ethernet 処理

影響: 悪意のある通信相手により Ethernet ヘッダより短い Ethernet フレームを受信した場合、受信バッファサイズ以上の領域を参照することで、KASAGO が動作停止する可能性があります。

補足: 正常な機器により送信された Ethernet フレームが受信時エラーとなり本現象に合致するデータ受信となった場合、通常は FCS のチェックでエラーとなるため、KASAGO へデータ送信される事はありません。

回避策: Ethernet コントローラまたはドライバにより Ethernet 規格以下のフレーム(最小ペイロード 46Byte を含む 60Byte 以下)および FCS エラーとなった Ether フレームを破棄する。

【CVE-2020-11907】

概要: KASAGO は TCP のヘッダ部分でフレーム分割された Ether フレームを受信した場合、動作停止する可能性がある。

対象: KASAGO IPv4 Lite および KASAGO IPv4、KASAGO IPv6(Dual)内の TCP 処理

影響: 通信相手が送信した TCP ヘッダ内部でフラグメントのあるデータを受信した場合、フラグメントされた後半の TCP ヘッダ情報をアップデートしないまま TCP ヘッダ処理を実施するため、動作停止となる可能性があります。

補足 1: 正常な機器では、極端に小さい MTU(例: MTU=46)が設定されている場合などのケースを除き TCP ヘッダでフラグメントが発生するパケットを送信する事はありません。通常の機器はこのような非効率な(小さい MTU)設定を利用することはありません。

補足 2: 本脆弱性はドライバの分割受信が有効になっている場合発生いたしません。

回避策: “TM_USE_DRV_SCAT_RECV”を設定する(ドライバの分割受信を有効にする)[5]。

【CVE-2020-11908】

概要: DHCP Client 動作時、文字列コピー動作時に NULL 終端をしないため、NULL が出現するまでのメモリの情報が漏洩する可能性があります。

対象: Ver. 4.7.1.26 以前の KASAGO IPv4 および KASAGO IPv6 に含まれる DHCP/Bootp クライアントの情報を利用するアプリケーション

影響: DHCP サーバによってオプションオーバーロード DHCP オプションを含むパケットを受信した後、情報が NULL 終端しない。これによりアプリケーションが該当文字列を参照する際にバッファをオーバーして情報を取得し、その情報を漏洩してしまう可能性があります。
NULL 終端されていないバッファは ttUserBtEntry 構造体中にある以下メンバです。

- btuBootSname TFTP サーバ name
- btuBootFileName ブート ファイル名
- btuDomainName ドメイン名

これらのメンバをアプリケーションから参照しない場合は問題発生しません。
本構造体は以下に示す KASAGO の API によりアプリケーションへ返却されます。

- tfConfGetBootEntry()

補足: KASAGO 内部処理では、“ttUserBtEntry 構造体”の参照は正しく行われるため、本現象は発生いたしません。各メンバのバッファサイズ未満のデータを受け取った場合にはバッファ全体が NULL 初期化されているため、この不具合は発生しません。

回避策: 最新バージョン(Ver6.0.1.33)の利用
アプリケーションにて各バッファサイズをチェックした上でデータを扱う。

---

[5] ドライバ分割受信を有効にする場合(TM_USE_DRV_SCAT_RECV の有効化)でもドライバ部分に修正は必要ありません。

各バッファサイズについては trsocket.h の以下のマクロで定義されております。

- btuBootSname　　TM_BOOTSNAME_SIZE　　64
- btuBootFileName　　TM_BOOTFILENAME_SIZE　128
- btuDomainName　　TM_FQDN_MAX_LEN　　252

【CVE-2020-11909】

概要:　異常な IP パケットのオプションを検出せず正常なパケットとして処理を行うため、動作不正となる可能性がある。

対象:　KASAGO IPv4 Lite および KASAGO IPv4、KASAGO IPv6(Dual)の IP 処理

影響:　悪意ある通信相手から送信された不正な Length(0)を持つ LSRR、SSRR オプションを含む IP パケットを受信した場合、IP 転送処理で悪意ある通信相手から送信されたオプションヘッダが不正なパケットの受信データを用いて処理が継続し、動作不正となる可能性があります。

回避策:　tfSetTreckOptions()で TM_OPTION_IP_FORWARDING を設定しない(IP 転送を有効にしない)

【CVE-2020-11910】

概要:　不正な ICMP パケットを排除できず、自身の MTU 値が不正となり動作不正となる可能性がある。

対象:　KASAGO IPv4 Lite および KASAGO IPv4、KASAGO IPv6(Dual)の ICMP 処理

影響:　悪意ある通信相手から送信された不正な ICMP パケットを受信した場合、受信データ外のバッファから MTU 値設定されるため通信障害が発生する可能性があります。

補足:　対象となる ICMP パケットは、ICMP のタイプ 3、コード 4 が選択されデータが存在せずにチェックサムだけが含まれる ICMP パケット

回避策:　最新バージョン(Ver6.0.1.33)における回避策は御座いません。
パッチ適用をご検討ください。

【CVE-2020-11911】

概要:　不正な ICMP のネットマスク変更応答を排除できず、自身のネットマスクを変更するため、動作不正となる可能性がある。

対象:　KASAGO IPv4 Lite および KASAGO IPv4、KASAGO IPv6(Dual)の ICMP 処理

影響:　悪意ある通信相手から KASAGO からのネットマスク変更要求の ICMP を送信していないにも関わらずットマスク変更応答を持った ICMP パケットを送信した場合にネットマスク変更を実行し正常な通信が不可能となる可能性があります。

回避策:　最新バージョン(Ver6.0.1.33)における回避策は御座いません。
パッチ適用をご検討ください。

【CVE-2020-11912】

概要: KASAGO は不正なヘッダを持つオプションを持つ TCP パケットを排除できず、バッファ外のデータを用いて処理を実行するため動作不正となる可能性がある。

対象: KASAGO IPv4 Lite および KASAGO IPv4、KASAGO IPv6(Dual)の TCP 処理

影響: 悪意ある通信相手から TCP ヘッダにて TimeStamp オプションまたは SACK オプションが有効だが実際のオプションデータを持たない TCP パケットを受信した場合、受信データ長を超えた領域から情報を取得するため、動作不正となる可能性があります。

回避策: 最新バージョン(Ver6.0.1.33)における回避策は御座いません。
パッチ適用をご検討ください。

【CVE-2020-11913】

概要: IPv6 ヘッダの後に続くペイロードデータが無いパケットを受信したときに、動作不正となる可能性がある。

対象: KASAGO IPv6(Dual)内の IPv6 処理

影響: 悪意ある通信相手が送信した IPv6 ヘッダの後に続くペイロードデータが無いパケットを受信したときに、実際にペイロードデータがあることを確認せずに、IPv6 ヘッダの次ヘッダに設定されたペイロード処理を実施し、受信データ長を超えた領域から情報を取得するため、動作不正となる可能性がある。

回避策: 最新バージョン(Ver6.0.1.33)における回避策は御座いません。
パッチ適用をご検討ください。

【CVE-2020-11914】

概要: 不正な ARP 情報を持つ Ether フレームを排除できず不正な通信相手にデータ送信する可能性がある。

対象: KASAGO IPv4 Lite および KASAGO IPv4、KASAGO IPv6(Dual)の ARP 処理

影響: 悪意のある通信相手により最低データサイズ(46Byte)を下回る ARP パケットが KASAGO に渡されたとき、受信データ範囲外のデータを参照し ARP テーブルを作成するため、不正な通信相手にデータ送信する可能性があります。

回避策: Ethernet コントローラまたはドライバにより Ethernet 規格以下のフレーム(最小ペイロード 46Byte を含む 60Byte 以下)をもつ Ether フレームを破棄する。

以上