2021 年 2 月 4 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しました事、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、お手数をお掛け致しますが、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 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-2020-27336			〇 (IPv6)		Ver6.0.1.33pa以前のバージョン
CVE-2020-27337			〇 (ICMPv6)		Ver6.0.1.33pa以前のバージョン
CVE-2020-11897				〇	Ver6.0.1.33pa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.pa)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」又は「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-2020-27336】

概要: IPv6 フレームに拡張ヘッダ Hop-by-Hop Options header 又は、拡張ヘッダ Destination Options header があり、かつ、そのオプション内に不正なオプションデータがある場合、動作停止する可能性があります。

対象: KASAGO IPv6 の IPv6 処理

影響: 悪意ある通信対象から意図的に拡張ヘッダ長を 1 バイト超えた部分にオプションサイズがある不正なオプションを持つ拡張ヘッダ Hop-by-Hop Options header 又は、拡張ヘッダ Destination Options header を含む IPv6 フレームを受信した場合、拡張ヘッダ領域を超えた 1 バイトをアクセスします。さらに、その拡張ヘッダがフレーム最後の部分だった場合、受信フレーム範囲外の 1 バイトをアクセスします。そのため、動作停止する可能性があります。

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

【CVE-2020-27337】

概要: ICMPv6 フレームのエラーカテゴリである Packet too Big (パケット過大) フレームを受信した場合、不正な受信フレームを排除できず、正常な通信が不可能となったり、動作停止する可能性があります。

対象: KASAGO IPv6 の ICMPv6 処理

影響: 悪意ある通信対象から意図的に以下の条件に合う ICMPv6 フレームのエラーカテゴリフレーム Packet too Big (パケット過大) を受信した場合、ルーティング拡張ヘッダの範囲外でも、エラー原因となったフレームのルーティング拡張ヘッダ先頭+(残りセグメント*16)の位置の値を IPv6 ルーティングノードのアドレスとして処理してしまいます。その誤った IPv6 アドレスがルーティング情報に存在する場合、その IPv6 アドレスの MTU を変更することがありました。また、エラー情報を発生したソケットに通知しないことがあり、正常な通信が不可能となる場合があります。

＜条件＞

1)エラー原因となったフレームの IPv6 ヘッダオプションにルーティング拡張ヘッダある

2)ルーティング拡張ヘッダのルーティングタイプが 0 で、ルーティング拡張ヘッダのサイズを超える残りセグメント数

3)ルーティング拡張ヘッダの次ヘッダが、カプセル化セキュリティーペイロード(ESP)、ICMPv6、TCP 又は UDP の値

さらに、エラー原因となったフレームのルーティング拡張ヘッダ先頭+(残りセグメント*16)の位置より 2 バイトの値が、0xFE 0x80 の場合、エラー原因となったフレームのルーティング拡張ヘッダ先頭+(残りセグメント*16)+4 の位置に、4 バイトのスコープ ID を書き込むためメモリを破壊することがあり、動作停止する可能性があります。

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

【CVE-2020-27338】

概要: DHCPv6 サーバより非臨時アドレス・アイデンティティ・アソシエーション (IA_NA, Identity Association for Non-temporary Addresses, 3)オプションを含む Reply、又は、Advertise フレームを受信した際、不正なオプションを排除できず、動作停止などが発生する可能性があります。

対象: KASAGO DHCPv6 クライアント オプション

影響: 悪意ある DHCPv6 サーバから意図的に DHCPv6 の非臨時アドレス・アイデンティティ・アソシエーション (IA_NA, Identity Association for Non-temporary Addresses, 3)オプションを含む Reply、又は、Advertise フレームに、非臨時アドレス・アイデンティティ・アソシエーション・オプションのオプションサイズを超えるオプションデータを持つフレームを受信した場合、サイズを確認せずにオプション以外の部分をオプションとして処理したり、フレーム範囲外をそのオプションとして処理することがあります。この動作により誤ったアドレスをレンタルされた IPv6 アドレスとして認識する可能性があり、正常な通信が不可能となったり、動作停止などが発生する可能性があります。

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

以上