

2022 年 2 月 10 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、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
- KASAGO IPv4 Light
- KASAGO mobile IPv6

脆弱性に影響を受ける製品に○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 mobile IPv6	該当バージョン
CVE-2022-43501	○	○	○	○	Ver6.0.1.33.pa.1 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、過去バージョン(Ver6.0.1.33pa.1以前)における回避策について説明します。(最新バージョンVer6.0.1.34では本問題は解決済みです)。「概要」欄中の「悪意ある通信対象」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-2022-43501】

概要:悪意ある通信対象に現在および将来のTCP接続初期シーケンス番号(ISN)を特定され、既存TCP接続を乗っ取られたり、将来のTCP接続を偽装される可能性があります。

対象:KASAGO IPv4、IPv6のTCP/IP処理

影響:TCP/IP通信において、自身がTCP/IP接続を実施する場合、TM_USE_TCP_128BIT_RANDOM_ISSマクロを指定すれば問題ありませんが、相手より接続された場合、TM_USE_TCP_128BIT_RANDOM_ISSマクロを指定してもRFC6528に定義された方法で初期シーケンス番号を作成せず、KASAGO独自のランダム取得関数を使用して作成するため、ランダム性が低くなり、TCP接続の初期シーケンス番号(ISN)を特定される可能性があります。

回避策:過去バージョン(Ver6.0.1.33pa.1以前)における回避策は御座いません。パッチ適用または最新バージョンVer6.0.1.34へのバージョンアップをお願い致します。

(バージョンアップ、またパッチの提供には条件がございます。別途お問い合わせください)

以上

以上