アイホン株式会社　＞　脆弱性に関する情報

IP ネットワーク対応インターホン IXG システム
攻撃を受けた際に、本商品が不正に操作される、本商品内のデータの流出や商品機能の一部が失われるなどの脆弱性

公開日　2024 年 10 月 16 日
最終更新日　2024 年 10 月 18 日

■概要
IP ネットワーク対応インターホン IXG システムについて脆弱性が存在することが判明しました。
この脆弱性を悪用された場合、ネットワーク経由でアクセス可能な第三者よって、データの閲覧・改ざん・削除、不正な操作が行われる可能性があります。なお、当攻撃は極めて専門性の高い技術が必要であることから、本商品の発売後、当攻撃を要因とした被害発生の報告は一切ございません。

■JPCERT/CC による脆弱性分析結果
1. CVE-2024-31408
CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 基本値 8.0
2. CVE-2024-39290
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値 6.5
3. CVE-2024-45837
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N 基本値 5.4

■対象商品及び対象バージョン
・対象商品：
カメラ付ゲート端末(IXG-DM7)
ゲートウェイアダプター(IXGW-GW、IXGW-TGW)
リレーアダプター(IXGW-LC)
IXG システム支援ソフト(IXG Support Tool)

・対象バージョン：
1. CVE-2024-31408、CVE-2024-39290
・IXGW-GW、IXGW-TGW：Ver3.01 およびそれ以前のすべてのバージョン
・IXG-DM7、IXGW-LC：Ver3.00 およびそれ以前のすべてのバージョン
※IXG システム支援ソフトは対象外
２. CVE-2024-45837
・IXGW-GW、IXGW-TGW：Ver3.01 およびそれ以前のすべてのバージョン
・IXG-DM7、IXGW-LC：Ver3.00 およびそれ以前のすべてのバージョン
・IXG システム支援ソフト：Ver.5.0.2.0 およびそれ以前のすべてのバージョン

・対象バージョンの確認方法：
対象商品により以下の手順で確認が可能です。

○IXG システム支援ソフトの場合
① IXG システム支援ソフトを開きメニューバーにある「ヘルプ」より「バージョン情報」を選択します。
② バージョン情報の画面より IXG システム支援ソフトのバージョンを確認します。

○上記以外の対象商品の場合
① IXG システム支援ソフトのインストーラをダウンロードしご使用の PC へインストールします。
② IXG システム支援ソフトをインストールした PC を対象商品のネットワークに接続します。
③ IXG システム支援ソフトを起動し、メニューバーにある「設定取得・反映」より「端末検索」を選択します。
④ 「検索開始」ボタンを押下し、「端末リスト」にある「ファームウェア」の欄より、対象商品のバージョンを確認します。
※IXG システム支援ソフトの使用方法は対象商品の商品ページ内にある「IXG システム支援ソフト設定説明書(施工モード) (Ver.5.0.0.0 以降) 」をご確認ください。

(商品ページは「商品情報ダウンロードページ」より検索することができます)

■脆弱性の説明
権限を持たない第三者によるネットワーク経由での不正アクセスによりデータの閲覧・改ざん・削除、不正な操作が行われるなどの脆弱性になります。

■脆弱性がもたらす脅威
対象商品への攻撃が成功すると、悪意のある第三者によって完全に制御されてしまう可能性があります。
これにより、悪意のある第三者から不正プログラムのインストール、データの閲覧・変更・削除など、システム管理者の権限でインターホンが操作される可能性があります。

■対策方法
対策済みファームウェアにアップデートを行う。
2024 年 8 月 27 日より対策済みファームウェアを配布しております。
「商品情報ダウンロードページ」より商品ページを検索後、対策済みファームウェアをダウンロードして頂き、IXG システム支援ソフトより対象商品のアップデートをお願い致します。

■関連情報
・JVN#41397971 アイホン製 IP ネットワーク対応インターホン IX システム、IXG システムおよびシステム支援ソフトにおける複数の脆弱性
・CVE-2024-31408/CVE-2024-39290/CVE-2024-45837
・ホームページへの掲載：
https://www.aiphone.co.jp/sustainability/product-security/psirt/vulnerability/2024/20241016_2.html

■謝辞

この脆弱性情報は、次の方が開発者に報告し、対象商品利用者への周知を目的に、開発者が IPA に報告し、JPCERT/CC が開発者との調整を行いました。

・報告者: Vera Mens of Claroty Research - Team82

■更新履歴

2024.10.16　脆弱性情報ページを公開しました。

2024.10.18　関連情報「JVN# 41397971」「CVE-2024-31408/CVE-2024-39290/CVE-2024-45837」を追加しました。

■連絡先

お問合せ頂くには、「商品に関するお問い合わせフォーム」よりお問合せください。