MELSEC iQ-R シリーズ及び iQ-F シリーズの EtherNet/IP ユニット並びに EtherNet/IP 設定ツールにおける複数の脆弱性

公開日 2023 年 6 月 1 日
三菱電機株式会社

■概要

MELSEC iQ-R シリーズ及び iQ-F シリーズの EtherNet/IP ユニット並びに EtherNet/IP 設定ツールにおいて、複数の脆弱性が存在することが判明しました。

EtherNet/IP ユニットの FTP 機能のパスワードの扱いが不適切なため、権限のない攻撃者が、FTP 接続を行い、認証を回避することにより、不正にログインする可能性があります。(CVE-2023-2060、CVE-2023-2061、CVE-2023-2062)

また、EtherNet/IP ユニットの FTP 機能は、ファイルのアップロード・ダウンロードを制限しないため、攻撃者が情報の漏えいや改ざん・削除、破壊を行える可能性があります。さらに、攻撃者が、更なる攻撃に悪用できる可能性があります。(CVE-2023-2063)

この脆弱性の影響を受ける製品名およびバージョンを以下に示しますので、軽減策・回避策の実施をお願いいたします。

■CVSS スコア [1]

CVE-2023-2060	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	基本値:7.5
CVE-2023-2061	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	基本値:6.2
CVE-2023-2062	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	基本値:6.2
CVE-2023-2063	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	基本値:6.3

■該当製品の確認方法

影響を受ける製品の形名、およびバージョンは以下の通りです。

形名	バージョン	説明
RJ71EIP91	すべてのバージョン	MELSEC iQ-R シリーズ EtherNet/IP ユニット
SW1DNN-EIPCT-BD	すべてのバージョン	RJ71EIP91 用 EtherNet/IP 設定ツール
FX5-ENET/IP	すべてのバージョン	MELSEC iQ-F シリーズ EtherNet/IP ユニット
SW1DNN-EIPCTFX5-BD	すべてのバージョン	FX5-ENET/IP 用 EtherNet/IP 設定ツール

■脆弱性の説明

該当製品には、以下の脆弱性が存在します。

・EtherNet/IP ユニットの FTP 機能には、脆弱なパスワードの要求(CWE-521)[2]により、パスワードに対する辞書攻撃や通信の盗聴によって取得したパスワードを用いて、認証を回避することが可能な脆弱性(CVE-2023-2060)があります。

・EtherNet/IP ユニットの FTP 機能には、ハードコードされたパスワードの使用(CWE-259)[3]により、ハードコーディングされたパスワードを取得することによって、認証を回避することが可能な脆弱性(CVE-2023-2061)があります。

・EtherNet/IP 設定ツールには、パスワードフィールドのマスキングの欠如(CWE-549)[4]により、パスワードが表示されるため、表示されたパスワードを用いて、認証を回避することが可能な脆弱性(CVE-2023-2062)があります。

・EtherNet/IP ユニットの FTP 機能には、危険なタイプのファイルの無制限アップロード(CWE-434)[5]により、ファイルのアップロード・ダウンロードが可能であり、情報の漏えいや改ざん・削除、破壊の脆弱性(CVE-2023-2063)があります。

■脆弱性がもたらす脅威

権限のない攻撃者が FTP でユニットに接続し、認証を回避して不正にログインする可能性があります。また、攻撃者は、ログイン後に、自由にファイルのアップロード・ダウンロードを行い、通信設定を閲覧したり、改ざん・削除及び破壊することができます。改ざん内容によっては、ユニットが再起動後に通信が停止したり意図しない通信を行うほか、更なる攻撃の起点となる可能性があります。

■対策方法

軽減策・回避策にて対応をお願いいたします。

■軽減策・回避策

本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。

・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止してください。

・当該製品を LAN 内で使用し、信頼できないネットワークやホストからのアクセスをファイアウォールでブロックしてください。

・当該製品を使用する LAN に信頼できないデバイスが接続されないように、物理的なアクセスを制限してください。

・FTP を使用し、直接ファイルのアップロード・ダウンロードすることは避け、EtherNet/IP 設定ツールを使用してください。かつ、ダウンロードしたファイルを EtherNet/IP 設定ツール以外で開かないでください。

・FX5-ENET/IP においては、IP フィルタ機能を使用し、信頼できないホストからのアクセスをブロックしてください。IP フィルタ機能については、以下のマニュアルを参照ください。

---

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html

2 https://cwe.mitre.org/data/definitions/521.html

3 https://cwe.mitre.org/data/definitions/259.html

4 https://cwe.mitre.org/data/definitions/549.html

5 https://cwe.mitre.org/data/definitions/434.html

MELSEC iQ-F FX5 ユーザーズマニュアル(Ethernet 通信編)「12.1 IP フィルタ機能」

■謝辞
本脆弱性をご報告いただいた、Iie Karada 様に感謝いたします。

■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。

〈お問い合わせ | 三菱電機 FA〉
https://www.mitsubishielectric.co.jp/fa/support/purchase/index.html