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
最終更新日 2024 年 10 月 31 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。

■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	該当 CVE 番号	説明
RJ71EIP91	すべてのバージョン	CVE-2023-2060 CVE-2023-2061 CVE-2023-2063	MELSEC iQ-R シリーズ EtherNet/IP ユニット
FX5-ENET/IP	すべてのバージョン	CVE-2023-2060 CVE-2023-2061 CVE-2023-2063	MELSEC iQ-F シリーズ EtherNet/IP ユニット
SW1DNN-EIPCT-BD	ソフトウェアバージョン"1.01B"以前	CVE-2023-2062	RJ71EIP91 用 EtherNet/IP 設定ツール
SW1DNN-EIPCTFX5-BD	ソフトウェアバージョン"1.01B"以前	CVE-2023-2062	FX5-ENET/IP 用 EtherNet/IP 設定ツール

<バージョンの確認方法>

・RJ71EIP91 : 「MELSEC iQ-R ユニット構成マニュアル」の「付 1 製造情報・ファームウェアバージョン」を参照ください。

・SW1DNN-EIPCT-BD : 「MELSEC iQ-R EtherNet/IP ユニットユーザーズマニュアル(応用編)」の「3.4 ソフトウェアバージョンの確認方法」を参照ください。

・FX5-ENET/IP : 「MELSEC iQ-F FX5 EtherNet/IP ユニットユーザーズマニュアル」の「付 4 バッファメモリ」の「バッファメモリ詳細」の「ファームウェアバージョン」を参照ください。

・SW1DNN-EIPCTFX5-BD : 「MELSEC iQ-F FX5 EtherNet/IP ユニットユーザーズマニュアル」の「8.3 ソフトウェアバージョンの確認方法」を参照ください。

■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。

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

■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。

■お客様での対応

脆弱性の影響を受ける形名およびバージョンの製品をお使いのお客様は以下の対応をお願いいたします。

形名	対応
RJ71EIP91	対策版のリリース予定はございませんので、軽減策・回避策にて対応をお願いいたします。 併せて、後継機種である CC-Link IE TSN Plus マスタ・ローカルユニット RJ71GN11-EIP への移行もご検討ください。
FX5-ENET/IP	軽減策・回避策にて対応をお願いいたします。
SW1DNN-EIPCT-BD	下記サイトから、次項に記載の対策済バージョンをダウンロードし、アップデートしてください。 https://www.mitsubishielectric.co.jp/fa/download/index.html
SW1DNN-EIPCTFX5-BD	下記サイトから、次項に記載の対策済バージョンをダウンロードし、アップデートしてください。 https://www.mitsubishielectric.co.jp/fa/download/index.html

■製品での対応

対策済の製品およびバージョンは、以下となります

形名	対策済のバージョン
SW1DNN-EIPCT-BD	ソフトウェアバージョン”1.02C”以降
SW1DNN-EIPCTFX5-BD	ソフトウェアバージョン”1.02C”以降

■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。

〈RJ71EIP91 および FX5-ENET/IP 共通〉

・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。

〈RJ71EIP91 ファームウェアバージョン”06”以降〉

・ファームウェアバージョン”06”以降では、FTP 機能を無効化することが可能です。EtherNet/IP Configuration Tool で設定を行うとき以外は、外部からの不正なアクセスを防止するために、Ethernet/IP Configuration Tool 接続許可変更機能にて接続を「禁止」に設定し、EtherNet/IP ユニットの FTP 機能を無効にしてください。設定手順の詳細は、以下のマニュアルを参照してください。なお、ファームウェアバージョン”06”より前の版から、ファームウェアバージョン”06”以降の版へのアップデートはできません。
　MELSEC iQ-R EtherNet/IP ユニットユーザーズマニュアル（応用編）「1.3 Ethernet/IP Configuration Tool 接続許可変更機能」

〈FX5-ENET/IP〉

・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。
　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」

〈FX5-ENET/IP ファームウェアバージョン”1.106”以降〉

・ファームウェアバージョン”1.106”以降では、FTP 機能を無効化することが可能です。EtherNet/IP Configuration Tool for FX5-ENET/IP で設定を行うとき以外は、外部からの不正なアクセスを防止するために、ツール接続設定変更機能にて接続を「禁止」に設定し、EtherNet/IP ユニットの FTP 機能を無効にしてください。設定手順の詳細は、以下のマニュアルを参照してください。
　MELSEC iQ-F FX5 EtherNet/IP ユニットユーザーズマニュアル「付 4 バッファメモリ」の「バッファメモリ詳細」の「ツール接続設定変更機能」

〈SW1DNN-EIPCT-BD および SW1DNN-EIPCTFX5-BD 共通〉

・RJ71EIP91 および FX5-ENET/IP において、上記の軽減策・回避策を実施ください。
・信頼できるユーザにのみログイン又はリモートログインを許可してください。
・当該製品を使用中に、他者に背後から覗かれないようにしてください。
・当該製品を使用中に離席する場合には、パソコンをロックし、他者が使用できないようにしてください。
・当該製品を使用するパソコンを 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ブロックしてください。
・当該製品を使用するパソコンならびに当該製品と通信可能なパソコンおよびネットワーク機器への物理的なアクセスを制限してください。
・当該製品を使用するパソコンおよび当該製品と通信可能なパソコンにウイルス対策ソフトを搭載してください。
・信頼できないファイルを開いたり、信頼できないリンクをクリックしないでください。

■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

■更新履歴
2024 年 10 月 31 日
・「該当製品の確認方法」に製品の<バージョンの確認方法>を追記しました。
FX5-ENET/IP、SW1DNN-EIPCTFX5-BD
・「お客様での対応」において、製品の対応を修正しました。
SW1DNN-EIPCTFX5-BD
・「製品での対応」に対策済みの製品を追記しました。
SW1DNN-EIPCTFX5-BD
・「軽減策・回避策」をバージョンごとの説明に分け、製品のバージョン情報を記載しました。
FX5-ENET/IP ファームウェアバージョン”1.106”以降

2024 年 4 月 25 日
・「対策方法」を「お客様での対応」と「製品での対応」に分けました。
・「製品での対応」に対策済みの製品を記載しました。
SW1DNN-EIPCT-BD
・「軽減策・回避策」を該当製品ごとの説明に分け、製品のバージョン情報を記載しました。
RJ71EIP91 ファームウェアバージョン”06”以降