MELSEC-F シリーズ基本ユニットにおける認証回避の脆弱性

公開日 2023 年 6 月 29 日
三菱電機株式会社

■概要

MELSEC-F シリーズ基本ユニットに、認証回避の脆弱性が存在することが判明しました。攻撃者は、該当製品に対して不正なパケットを送信することにより、当該製品に対して不正アクセスすることができる可能性があります。(CVE-2023-2846)

■CVSS スコア [1]

CVE-2023-2846 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値 7.5

■該当製品の確認方法

影響を受ける製品とバージョンは以下の通りです。ただし、Ethernet 通信用特殊アダプタ FX3U-ENET-ADP 又は Ethernet インタフェースブロック FX3U-ENET(-L)を使用する場合に、本脆弱性の影響を受けます。

シリーズ	製品形名	バージョン
MELSEC-F シリーズ	FX3U-xMy/z x=16,32,48,64,80,128, y=T,R, z=ES,ESS,DS,DSS	全バージョン
	FX3U-32MR/UA1, FX3U-64MR/UA1	
	FX3U-32MS/ES, FX3U-64MS/ES	
	FX3UC-xMT/z x=16,32,64,96, z=D,DSS	
	FX3UC-16MR/D-T, FX3UC-16MR/DS-T	
	FX3UC-32MT-LT, FX3UC-32MT-LT-2	
	FX3G-xMy/z x=14,24,40,60, y=T,R, z=ES,ESS,DS,DSS	
	FX3GC-32MT/D, FX3GC-32MT/DSS	
	FX3S-xMy/z x=10,14,20,30, y=T,R, z=ES,ESS,DS,DSS	
	FX3S-30My/z-2AD y=T,R, z=ES,ESS	

■脆弱性の説明

MELSEC-F シリーズ基本ユニットには、Capture-replay による認証回避(CWE-294[2])による、認証回避の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者は、該当製品に対して不正なパケットを送信することにより、パスワード/キーワード設定を解除し、当該製品に対して不正アクセスすることができ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。
・当該製品および当該製品が接続された LAN への物理的なアクセスを制限してください。

■謝辞

本脆弱性をご報告いただいた、浙江大学 307LAB の Chun Liu 様、Xin Che 様、Ruilong Deng 様、Peng Cheng 様、Jiming Chen 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

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/294.html