MELFA FR シリーズおよび CR シリーズ並びに ASSISTA のロボットコントローラにおけるサービス拒否(DoS)の脆弱性

公開日 2021 年 1 月 21 日
最終更新日 2021 年 5 月 18 日
三菱電機株式会社

■概要

当社産業用ロボット MELFA FR シリーズおよび CR シリーズ並びに協働ロボット ASSISTA のロボットコントローラにおいて、リソース管理の問題(CWE-399)によるサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者からロボットコントローラの Ethernet ポートに対して短時間に大量に送信されたパケットを受信すると、ロボットプログラムの実行および通信が DoS 状態に陥る可能性があります。なお、DoS 状態に陥った際に、エラーが発生する場合があります。(CVE-2021-20586)

この脆弱性の影響を受ける製品シリーズ名およびファームウェアバージョンを以下に示します。

■CVSS スコア

CVE-2021-20586 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5

■該当製品の確認方法

MELFA FR シリーズおよび CR シリーズ並びに ASSISTA のロボットコントローラにおいて、表 1 の型名とファームウェアバージョンが影響を受けます。ファームウェアバージョンの確認方法は次項を参照ください。

表 1. 該当製品

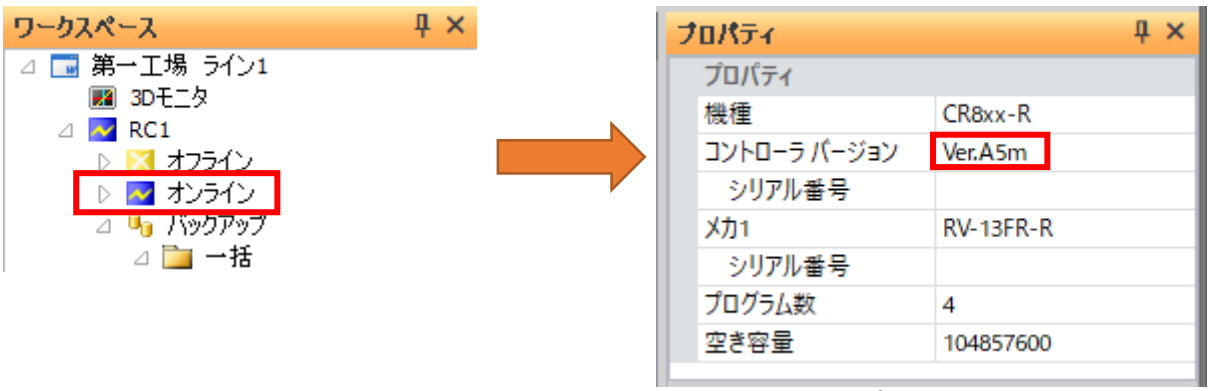
シリーズ	型名	コントローラ型式	ファームウェアバージョン
MELFA FRシリーズ	RV-□FR○■△-D-◎	CR800-□V○D	全バージョン
	RH-□FRH○☆△-D-◎	CR800-□HD	
	RH-□FRHR○☆△-D-◎	CR800-□HRD	
	RV-□FR○■△-R-◎	R16RTCPU + CR800-□V○R	
	RH-□FRH○☆△-R-◎	R16RTCPU + CR800-□HR	
	RH-□FRHR○☆△-R-◎	R16RTCPU + CR800-□HRR	
	RV-□FR○■△-Q-◎	Q172DSRCPU + CR800-□V○Q	
	RH-□FRH○☆△-Q-◎	Q172DSRCPU + CR800-□HQ	
	RH-□FRHR○☆△-Q-◎	Q172DSRCPU + CR800-□HRQ	
MELFA CRシリーズ	RV-8CRL-D-◎	CR800-CVD	
	RH-□CRH○☆-D-◎	CR800-CHD	
MELFA ASSISTA	RV-5AS-D-◎	CR800-05VD	

□:可搬質量(型名:2、3、4、6、7、12、13、20、コントローラ型式:02、03、04、06、07、12、13、20) ○:アーム長(型名 RV:L、LL もしくはブランク、型名 RH:35、40、45、55、60、70、85、100、コントローラ型式:L もしくはブランク) ■:ブレーキ使用(B もしくはブランク) ☆:上下ストローク(12、15、18、20、34、35、45) △:本体環境仕様(M、C、W もしくはブランク) ◎:特殊機番号(S**もしくはブランク)

■ファームウェアバージョンの確認方法

・RT ToolBox3 を使用する場合

ワークスペース画面(図 1(a)参照)の対象プロジェクトの[オンライン]部を選択すると、プロパティ画面(図 1(b)参照)にてファームウェアバージョンが確認できます。



(a)ワークスペース画面　　(b)プロパティ画面

図 1.RT ToolBox3 によるファームウェアバージョンの確認方法

・R32TB を使用する場合
タイトル画面(図 2 参照)にてファームウェアバージョンが確認できます。

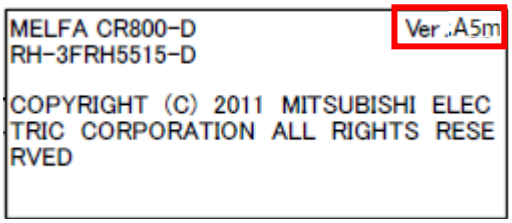


図 2. R32TB によるファームウェアバージョンの確認方法

・R56TBを使用する場合
バージョン画面(図3参照)にてファームウェアバージョンが確認できます。

図 3. R56TB によるファームウェアバージョンの確認方法

■脆弱性の説明
MELFA FR シリーズおよび CR シリーズ並びに ASSISTA のロボットコントローラにおいて、リソース管理の問題(CWE-399)によるサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威
攻撃者からロボットコントローラの Ethernet ポートに対して短時間に大量に送信されたパケットを受信すると、ロボットプログラムの実行および通信が DoS 状態に陥る可能性があります。なお、DoS 状態に陥った際に、エラーが発生する場合があります。エラーが発生した場合、復旧にはロボットコントローラの電源再投入が必要になります。

■対策方法
下記軽減策にて対応ください。

■軽減策
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。
・当該製品の IP フィルタ機能(※1)を使用し、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。

※1：IP フィルタ機能に対応したシリーズとファームウェアバージョンは以下となります。
＜シリーズとファームウェアバージョン＞
・MELFA FR シリーズ ： C2 版 以降
・MELFA CR シリーズ ： C2 版 以降
・MELFA ASSISTA ： C2 版 以降
＜対応済製品の入手方法＞
製品をご購入いただいた弊社の支社、代理店にご相談ください。

■謝辞
この問題をご報告いただいた Qi An Xin Group Inc. from China 社 Industrial Control Security Laboratory 殿に感謝いたします。

■お客様からのお問い合わせ先
お客様からのお問い合わせ先につきましては、製品をご購入いただいた弊社の支社、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
2021 年 5 月 18 日
「対策方法」を変更しました。
「軽減策」に IP フィルタ機能を追加しました。