MELFA SD/SQ シリーズおよび F シリーズの ロボットコントローラにおける認証回避の脆弱性

公開日 2023 年 1 月 26 日
三菱電機株式会社

■概要

産業用ロボット MELFA SD/SQ シリーズおよび F シリーズのロボットコントローラにおいて、アクティブ状態のデバッグコード(CWE-489)[1]による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、telnet による不正なログインを行い、ロボットコントローラへ不正にアクセスすることができます。(CVE-2022-33323)

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 [2]

CVE-2022-33323　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

MELFA SD/SQ シリーズおよび F シリーズ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

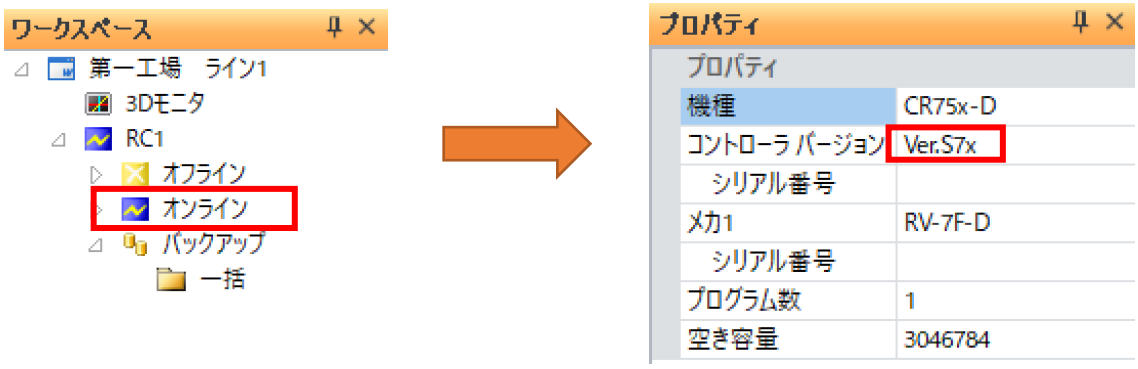
シリーズ	型名	コントローラ型式	ファームウェアバージョン
MELFA SD/SQシリーズ	RV-□SD○●■△-◎	CR□DA-◇◇◇△	S7x版 以前
	RH-□SDH○●■△-◎		
	RH-□SDHR○☆■△-◎		
	RV-□SQ○●■△-◎	CR□QA-◇◇◇△	R7x版 以前
	RH-□SQH○●■△-◎		
	RH-□SQHR○☆■△-◎		
MELFA Fシリーズ	RV-□F○■△-▲D-◎	CR◇◇◇-□VD	S7x版 以前
	RH-□FH○☆△-▲D-◎	CR◇◇◇-□HD	
	RH-□FHR○☆△-▲D-◎		
	RV-□F○■△-▲Q-◎	CR◇◇◇-□VQ	R7x版 以前
	RH-□FH○☆△-▲Q-◎	CR◇◇◇-□HQ	
	RH-□FHR○☆△-▲Q-◎		

□:可搬質量(型名:2、3、4、6、7、12、13、18、20、コントローラ型式(SD/SQ シリーズ:1、2、3、F シリーズ: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) ●:軸構成(J 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) ▲:コントローラのシリーズ(1 もしくはブランク) ◎:特殊機番号(S**もしくはブランク) ◇◇◇:コントローラのシリーズ名(SD/SQ シリーズ:701、711、721、731,、741、751、761、771、772、781、F シリーズ:750、751、760)

■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を確認できます。



(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

1 https://cwe.mitre.org/data/definitions/489.html

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

・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を確認できます。

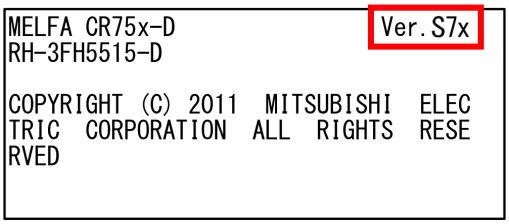


図 2. R32TB によるファームウェアバージョンの確認方法

・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を確認できます。

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 SD/SQ シリーズおよび F シリーズのロボットコントローラにおいて、アクティブ状態のデバッグコード(CWE-489)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、telnet による不正なログインを行い、ロボットコントローラへ不正にアクセスすることができます。

■対策方法

該当製品については、以下のファームウェアバージョンで対策済みです。

表 2. 対策済みファームウェアバージョン

シリーズ	型名	ファームウェアバージョン
MELFA SD/SQシリーズ	RV-□SD〇●■△-◎	S7y版 以降
	RH-□SDH〇●■△-◎	
	RH-□SDHR〇☆■△-◎	
	RV-□SQ〇●■△-◎	R7y版 以降
	RH-□SQH〇●■△-◎	
	RH-□SQHR〇☆■△-◎	
MELFA Fシリーズ	RV-□F〇■△-▲D-◎	S7y版 以降
	RH-□FH〇☆△-▲D-◎	
	RH-□FHR〇☆△-▲D-◎	
	RV-□F〇■△-▲Q-◎	R7y版 以降
	RH-□FH〇☆△-▲Q-◎	
	RH-□FHR〇☆△-▲Q-◎	

□、〇、☆、●、■、△、▲、◎：表 1 と同じです。

＜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。

■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。

■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