Authentication Bypass Vulnerability in Robot Controller of MELFA SD/SQ series and F-series

Release date: January 26, 2023
Mitsubishi Electric Corporation

■Overview

Authentication bypass vulnerability due to active debug code (CWE-489)[1] exists in robot controller of industrial robot MELFA SD/SQ series and F-series.An attacker can gain unauthorized access to a robot controller by performing an unauthorized telnet login. (CVE-2022-33323)

The product series names and firmware versions affected by this vulnerability are listed below.

■CVSS[2]

CVE-2022-33323 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score: 7.5

■Affected products

For MELFA SD/SQ series and F-series robot controllers,model names and firmware versions in Table 1 are affected. See the next section for how to check the firmware version.

Table 1. Affected Products

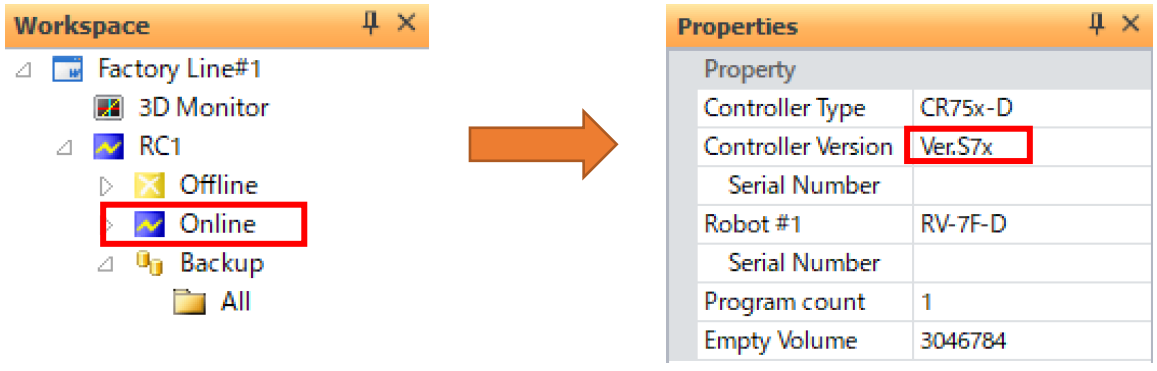
Series	Model name	Controller type	Firmware version
MELFA SD/SQ Series	RV-#SD$!%¥-@	CR#DA-***¥	S7x and prior
	RH-#SDH$!%¥-@		
	RH-#SDHR$&%¥-@		
	RV-#SQ$!%¥-@	CR#QA-***¥	R7x and prior
	RH-#SQH$!%¥-@		
	RH-#SQHR$&%¥-@		
MELFA F-Series	RV-#F$%¥-?D-@	CR***-#VD	S7x and prior
	RH-#FH$&¥-?D-@	CR***-#HD	
	RH-#FHR$&¥-?D-@		
	RV-#F$%¥-?Q-@	CR***-#VQ	R7x and prior
	RH-#FH$&¥-?Q-@	CR***-#HQ	
	RH-#FHR$&¥-?Q-@		

#: Load capacity (Model name: 2, 3, 4, 6, 7, 12, 13, 18, 20, Controller type (SD/SQ Series: 1, 2, 3, F-Series: 02, 03, 04, 06, 07, 12, 13, 20)) $:Arm length (Model name RV: L, LL or blank, Model name RH: 35, 40, 45, 55, 60, 70, 85, 100) !:Shaft configuration (J or blank) %:Using brakes (B or blank) &:Up and down strokes (12, 15, 18, 20, 34, 35, 45) ¥:Body environmental specifications (M, C, W or blank) ?:Series of controllers (1 or blank) @:Special machine number (S** or blank) ***: Series of controllers (SD/SQ Series: 701, 711, 721, 731, 741, 751, 761, 771, 772, 781, F-Series: 750, 751, 760)

■How to Check the Firmware Version

・When using RT ToolBox3

When you select the [Online] section of the target project on the workspace screen (see Fig. 1 (a)), you can check the firmware version on the properties screen (see Fig. 1 (b)).



(a)Workspase screen (b)Property screen

Figure 1. How to Check the Firmware Version with RT ToolBox3

1 https://cwe.mitre.org/data/definitions/489.html
2 https://www.first.org/cvss/v3.1/specification-document

・When using R32TB

The firmware version can be checked on the title screen (see Fig. 2).

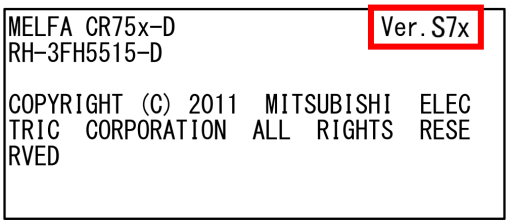


Figure 2. How to Check the Firmware Version with R32TB

・When using R56TB

The firmware version can be checked on the version screen (see Fig. 3).

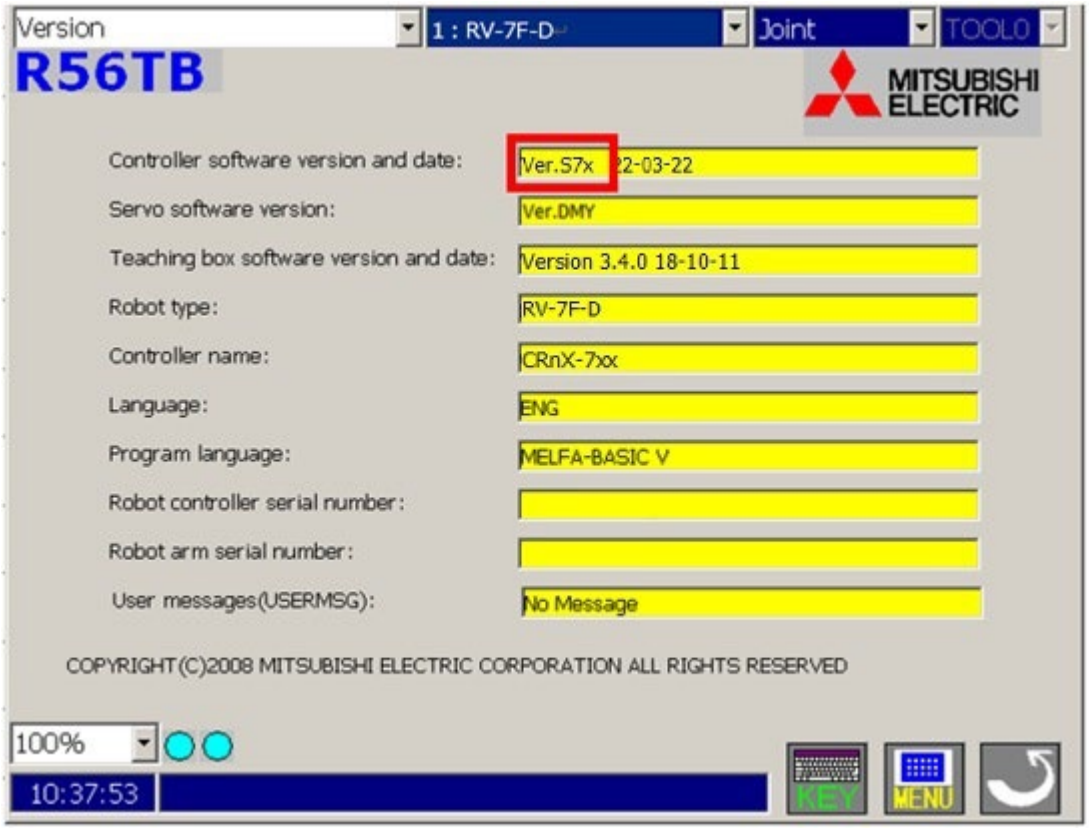


Figure 3. How to Check the Firmware Version

■Description

An authentication bypass vulnerability due to active debug code (CWE-489) exists in robot controller of MELFA SD/SQ series and F-series.

■Impact

An attacker can gain unauthorized access to a robot controller by performing an unauthorized telnet login.

■Countermeasures

The affected product has been fixed in the following firmware versions.

Table 2. Fixed firmware version

Series	Type name	Firmware version
MELFA SD/SQ Series	RV-#SD$!%¥-@	S7y or later
	RH-#SDH$!%¥-@	
	RH-#SDHR$&%¥-@	
	RV-#SQ$!%¥-@	R7y or later
	RH-#SQH$!%¥-@	
	RH-#SQHR$&%¥-@	
MELFA F-Series	RV-#F$%¥-?D-@	S7y or later
	RH-#FH$&¥-?D-@	
	RH-#FHR$&¥-?D-@	
	RV-#F$%¥-?Q-@	R7y or later
	RH-#FH$&¥-?Q-@	
	RH-#FHR$&¥-?Q-@	

#,$,&,!,%,¥,?,@:Same as Table 1.

<How to get the fixed versions>

Please contact your local Mitsubishi Electric representative.

■Mitigations

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:

・Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.

・Use within a LAN and block access from untrusted networks and hosts through firewalls.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

https://www.mitsubishielectric.com/en/index.html