Authentication Bypass, Information Disclosure and Information Tampering Vulnerabilities in Multiple FA Products

Release date: March 31, 2022
Last update date: May 31, 2022
Mitsubishi Electric Corporation

■Overview

Authentication bypass, information disclosure and information tampering vulnerabilities exist in multiple Mitsubishi Electric FA products. If these vulnerabilities are exploited by a malicious attacker, an unauthenticated attacker may be able to login to the products or the information in the products may be disclosed or tampered with. (CVE-2022-25155, CVE-2022-25156, CVE-2022-25157, CVE-2022-25158, CVE-2022-25159, CVE-2022-25160)

■CVSS

CVE-2022-25155	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	Base Score 5.9
CVE-2022-25156	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	Base Score 5.9
CVE-2022-25157	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N	Base Score 7.4
CVE-2022-25158	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N	Base Score 7.4
CVE-2022-25159	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	Base Score 5.9
CVE-2022-25160	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N	Base Score 6.8

■Affected products

The following products are affected:

Seies	Product name	Version
MELSEC iQ-F series	FX5U(C) CPU modules, All models	All versions
	FX5UJ CPU modules, All models	All versions
MELSEC iQ-R series	R00/01/02CPU	All versions
	R04/08/16/32/120(EN)CPU	All versions
	R08/16/32/120SFCPU	All versions
	R08/16/32/120PCPU	All versions
	R08/16/32/120PSFCPU	All versions
	R16/32/64MTCPU (*1)	All versions
	RJ71GN11-T2 (*2)	All versions
	RJ71GN11-EIP (*2)	All versions
	RJ71C24(-R2/R4)	All versions
	RJ71EN71	All versions
	RJ71GF11-T2 (*3)	All versions
	RJ71GP21(S)-SX (*3)	All versions
	RJ72GF15-T2	All versions
MELSEC Q series	Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU (*4)	All versions
	Q03/04/06/13/26UDVCPU	All versions
	Q04/06/13/26UDPVCPU	All versions
	QJ71C24N(-R2/R4)	All versions
	QJ71E71-100	All versions
	QJ72BR15 (*5)	All versions
	QJ72LP25(-25/G/GE) (*5)	All versions
MELSEC L series (*4)	L02/06/26CPU(-P), L26CPU-(P)BT	All versions
	LJ71C24(-R2)	All versions
	LJ71E71-100	All versions
	LJ72GF15-T2	All versions

*1 Only affected by CVE-2022-25157/25159/25160
*2 Only affected by CVE-2022-25155
*3 Only affected by CVE-2022-25157/25158
*4 Only affected by CVE-2022-25155/25156/25157/25158
*5 Only affected by CVE-2022-25155/25156

■Description

Multiple vulnerabilities below exist in multiple Mitsubishi Electric FA products.

CVE-2022-25155: Use of Password Hash Instead of Password for Authentication(CWE-836)
CVE-2022-25156: Use of Weak Hash(CWE-328)
CVE-2022-25157: Use of Password Hash Instead of Password for Authentication(CWE-836)
CVE-2022-25158: Cleartext Storage of Sensitive Information(CWE-312)
CVE-2022-25159: Authentication Bypass by Capture-replay(CWE-294)
CVE-2022-25160: Cleartext Storage of Sensitive Information(CWE-312)

■Impact

If these vulnerabilities are exploited by a malicious attacker, an unauthenticated attacker may be able to login to the products or the information in the products may be disclosed or tampered with.

■Countermeasures

Please carry out mitigations/workarounds.

■Mitigations/Workarounds

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

- When communicating via untrusted networks or hosts, encrypt the communication path by setting up a VPN.
- Use firewalls or IP filter function to restrict connections to the products and prevent access from untrusted networks or hosts. For details on IP filter function, refer to the following product manual.
  "12.1 IP Filter Function" in the MELSEC iQ-F FX 5 User's Manual (Ethernet Communication)
  "IP filter" of "1.13 Security" in the MELSEC iQ-R Ethernet User's Manual (Application)
  "IP Filter Function" of "6.2 Security Function" in the MELSEC iQ-R Motion Controller Programming Manual (Common)
  "IP filter" of "1.4 Security" in the MELSEC iQ-R CC-Link IE TSN User's Manual (Application)
  "IP filter" of "9.5 Security" in the MELSEC iQ-R CC-Link IE TSN Plus Master/Local Module User's Manual
  "14.3 IP Filter Function" in the Q Corresponding Ethernet Interface Module User's Manual (Basic)
  "14.3 IP Filter Function" in the MELSEC-L Ethernet Interface Module User's Manual (Basic)

■Acknowledgement

Mitsubishi Electric would like to thank the following Positive Technologies researchers who reported these vulnerabilities.
CVE-2022-25155: Anton Dorfman
CVE-2022-25156: Dmitry Sklyarov, Anton Dorfman
CVE-2022-25157: Anton Dorfman
CVE-2022-25158: Anton Dorfman, Iliya Rogachev
CVE-2022-25159: Anton Dorfman
CVE-2022-25160: Anton Dorfman, Artur Akhatov

■Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html

■Update history

May 31, 2022
Added MELSEC iQ-R/Q/L series to “Affected products”.
Added MELSEC iQ-R/Q/L series product manual information to “Mitigations/Workarounds”.