Denial of Service(DoS) and Remote Code Execution Vulnerability in MELSEC-Q/L Series Ethernet Interface Module and MELSEC iQ-R Series MES Interface Module

Release date: June 2, 2022
Mitsubishi Electric Corporation

■Overview

Denial of Service(DoS) and Remote Code Execution Vulnerability exists in Web function on MELSEC-Q Ethernet Interface Module and MELSEC-L Ethernet Interface Module, and REST Server function on MELSEC iQ-R MES Interface Module. A remote unauthenticated attacker may cause a denial of service (DoS) condition or execute malicious code on target products by sending specially crafted packets.(CVE-2022-25163)

The model names and firmware versions affected by this vulnerability are listed below. Please take measures based on the following Countermeasures or Mitigations/Worksarounds.

■CVSS

CVE-2022-25163 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score:8.1

■Affected products

Affected products and versions are below.

Series	Product Name	Function Name	Version
MELSEC-Q Series	QJ71E71-100	Web function	First 5 digits of serial number “24061” or prior.
MELSEC-L Series	LJ71E71-100	Web function	First 5 digits of serial number “24061” or prior.
MELSEC iQ-R Series	RD81MES96N	REST Server function	Firmware version “08” or prior

Please refer to the following manuals for how to check the serial number and version.

QJ71E71-100:

Q Corresponding Ethernet Interface Module User’s Manual (Basic) “Appendix 11 Checking the Serial Number and Function Version”

LJ71E71-100:

MELSEC-L Ethernet Interface Module User’s Manual (Basic) “Appendix 10 Checking the Serial Number, Function Version, and MAC address”

RD81MES96N:

MELSEC iQ-R Module Configuration Manual “Appendix 1 Checking Production Information and Firmware Version”

■Description

Denial of Service(DoS) and Remote Code Execution Vulnerability due to Improper Input Validation(CWE-20) exists in Web function on MELSEC-Q Ethernet Interface Module and MELSEC-L Ethernet Interface Module, and REST Sever function on MELSEC iQ-R MES Interface Module.

■Impact

A remote unauthenticated attacker may cause a DoS condition or execute malicious code on target products by sending specially crafted packets. A system reset is required for recovery from a denial of service (DoS) condition and remote code execution.

■Countermeasures

We have fixed the vulnerability at the following version.

Series	Product Name	Version
MELSEC-Q Series	QJ71E71-100	First 5 digits of serial number “24062” or later.
MELSEC-L Series	LJ71E71-100	First 5 digits of serial number “24062” or later.
MELSEC iQ-R Series	RD81MES96N	Firmware version “09” or later

■Mitigations/Workarounds

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

- Use a firewall, virtual private network (VPN), web application firewall (WAF), 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/fa/support/index.html