Information Disclosure, Information Tampering, and Denial of Service (DoS) Vulnerability in Mitsubishi Electric proprietary protocol communication and SLMP communication for FA products

Release date: February 5, 2026
Mitsubishi Electric Corporation

Overview

An information disclosure, information tampering, and denial of service (DoS) vulnerability exists in Mitsubishi Electric proprietary protocol communication and SLMP communication used in FA products. An attacker may be able to read device data or part of a control program from the affected product, write device data in the affected product, or cause a denial of service (DoS) condition on the affected product by sending a specially crafted packet containing a specific command to the affected product. (CVE-2025-15080)

CVSS[1]

CVE-2025-15080 CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N Base Score:8.8

Affected products

The following products are affected:

Series	Model name	Version
MELSEC iQ-R Series	R08/16/32/120PCPU	firmware versions "48" and prior

Description

An information disclosure, information tampering, and denial of service (DoS) vulnerability due to Improper Validation of Specified Quantity in Input (CWE-1284[2]) exists in Mitsubishi Electric proprietary protocol communication and SLMP communication used in the affected products.

Impact

An attacker may be able to read device data or part of a control program from the affected product, write device data in the affected product, or cause a denial of service (DoS) condition on the affected product by sending a specially crafted packet containing a specific command to the affected product.

Countermeasures for Customers

Customers using the affected products should follow the update procedure below to update the firmware to a fixed version described in "Countermeasures for Products."

[Update procedure]
Download the update file for the fixed version, the engineering software for firmware upgrade, and the manual from the following website.
https://www.mitsubishielectric.com/fa/download/index.html
For details on updating the firmware, see below.
・MELSEC iQ-R Module Configuration Manual "Appendix 2 Firmware Update Function"

Countermeasures for Products

The following products have been fixed.

Series	Model name	Version
MELSEC iQ-R Series	R08/16/32/120PCPU	firmware versions "49" or later

Mitigations / Workarounds

Mitsubishi Electric recommends the following mitigations to minimize the risk of exploitation of this vulnerability.
・Use a firewall or virtual private network (VPN) to prevent unauthorized access when internet access is required.
・Use the product within a LAN and block access from untrusted networks and hosts through a firewall.
・Use firewalls, IP filters, etc., to minimize connections to the product and prevent access from untrusted networks and hosts. For the IP filter function, refer to the following manuals.
"IP filter" in "1.13 Security" of the MELSEC iQ-R Ethernet User's Manual (Application)

[1] https://www.first.org/cvss/v4-0/specification-document

[2] https://cwe.mitre.org/data/definitions/1284.html

・Restrict physical access to the affected product and the LAN to which it is connected.

Contact information

Please contact your local Mitsubishi Electric representative.

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