Denial-of-Service (DoS) Vulnerability in MELSEC-Q Series CPU module

Release date: September 18, 2025
Mitsubishi Electric Corporation

Overview

Denial-of-Service (DoS) vulnerability exists in MELSEC-Q series CPU module when the user authentication function is enabled. The user authentication function is enabled by default only when settings are configured by GX Works2, which complies with the Cybersecurity Law of the People's Republic of China, and is normally disabled. A remote attacker may be able to cause an integer underflow by sending specially crafted packets to the affected product to stop Ethernet communication and the execution of control programs on the product. (CVE-2025-8531)

CVSS[1]

CVE-2025-8531 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H Base Score:6.8

Affected products

Affected products and versions are below.

Series	Model name	Version
MELSEC-Q Series	Q03/04/06/13/26UDVCPU	The first 5 digits of serial No. "24082" to "27081"
	Q04/06/13/26UDPVCPU	The first 5 digits of serial No. "24082" to "27081"

Description

Denial-of-Service (DoS) vulnerability exists in the MELSEC-Q series CPU module when the user authentication function is enabled, due to Improper Handling of Length Parameter Inconsistency (CWE-130[2]).

Impact

A remote attacker may be able to cause an integer underflow by sending specially crafted packets to the affected product to stop Ethernet communication and the execution of control programs on the product. A system reset of the product is required for recovery.

Countermeasures for Customers

Customers using the affected products and versions may are kindly requested to take the measures described in the “Mitigations / Workarounds” section.

We have released the fixed version as shown in Countermeasures for Products section, but updating the product to the fixed version is not available. Please consider migrating to the successor model, MELSEC iQ-R Series.

Countermeasures for Products

The following products have been fixed.

Series	Model name	Version
MELSEC-Q Series	Q03/04/06/13/26UDVCPU	The first 5 digits of serial No. "27082" or later
	Q04/06/13/26UDPVCPU	The first 5 digits of serial No. "27082" 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 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.
- Restrict physical access to the affected products, as well as to computers and network devices that can be connected to those products.

Contact information

Please contact your local Mitsubishi Electric representative.

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

1 https://www.first.org/cvss/v3.1/specification-document

2 https://cwe.mitre.org/data/definitions/130.html