Information Disclosure and Remote Code Execution Vulnerabilities in MELSEC-Q/L Series CPU Module

Release date: March 14, 2024
Mitsubishi Electric Corporation

Overview

Information disclosure and remote code execution vulnerabilities due to Incorrect Pointer Scaling (CWE-468[1]) and Integer Overflow or Wraparound (CWE-190[2]) exist in MELSEC-Q/L Series CPU modules. A remote attacker may be able to read arbitrary information from a target product or execute malicious code on a target product by sending a specially crafted packet. (CVE-2024-0802, CVE-2024-0803, CVE-2024-1915, CVE-2024-1916, CVE-2024-1917)

CVSS[3]

CVE-2024-0802	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score : 9.8
CVE-2024-0803	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score : 9.8
CVE-2024-1915	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score : 9.8
CVE-2024-1916	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score : 9.8
CVE-2024-1917	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score : 9.8

Affected products

The following products and firmware versions are affected:

Series	Product name	Firmware Version
MELSEC-Q Series	Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU	all versions
	Q03/04/06/13/26UDVCPU	all versions
	Q04/06/13/26UDPVCPU	all versions
MELSEC-L Series	L02/06/26CPU(-P), L26CPU-(P)BT	all versions

Description

The following five vulnerabilities exist in MELSEC-Q/L series CPU units.
- CVE-2024-0802: Information disclosure and remote code execution vulnerability due to Incorrect Pointer Scaling (CWE-468)
- CVE-2024-0803: Remote code execution vulnerability due to Integer Overflow or Wraparound (CWE-190)
- CVE-2024-1915: Remote code execution vulnerability due to Incorrect Pointer Scaling (CWE-468)
- CVE-2024-1916: Remote code execution vulnerability due to Integer Overflow or Wraparound (CWE-190)
- CVE-2024-1917: Remote code execution vulnerability due to Integer Overflow or Wraparound (CWE-190)

Impact

[CVE-2024-0802]
A remote attacker may be able to read arbitrary information from a target product or execute malicious code on a target product by sending a specially crafted packet.

[CVE-2024-0803, CVE-2024-1915, CVE-2024-1916, CVE-2024-1917]
A remote attacker may be able to execute malicious code on a target product by sending a specially crafted packet.

Countermeasures

Mitsubishi Electric will release a fixed version of the firmware in the near future.

Mitigations/Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities:
- Use a firewall, 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 product as well as to the personal computers and the network devices that can communicate with it.
- Install antivirus software on your personal computer that can access the affected product.

---

1 https://cwe.mitre.org/data/definitions/468.html
2 https://cwe.mitre.org/data/definitions/190.html
3 https://www.first.org/cvss/v3.1/specification-document

Acknowledgement

Mitsubishi Electric would like to thank Anton Dorfman (Positive Technologies) who reported these vulnerabilities.

Contact information

Please contact your local Mitsubishi Electric representative.

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