Denial of Service(DoS) and Malicious Code Execution Vulnerability in DHCP client function on MELSEC-Q Series C Controller Module

Release date: April 7, 2022
Mitsubishi Electric Corporation

■Overview

Denial of Service(DoS) and Malicious Code Execution Vulnerability exists in DHCP client function of VxWorks version 6.4, a real-time OS distributed by Wind River. A remote attacker may cause a denial of service (DoS) condition or execute malicious code on a target product by sending specially crafted packets.(CVE-2021-29998)

The model names and firmware versions of the MELSEC C Controller Module affected by this vulnerability are listed below.

■CVSS

CVE-2021-29998　CVSS:3.1 /AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H　Base Score: 9.0

■Affected products

Affected products and versions are below.

Module Name	Version
Q12DCCPU-V	First 5 digits of serial number are “24031” or prior.

Please refer to the manual of the affected product for how to check the serial number.

QCPU User's Manual (Hardware Design, Maintenance and Inspection) "Appendix 5 Checking Serial Number and Function Version"

■Description

Denial of Service(DoS) and Malicious Code Execution Vulnerability due to heap-based buffer overflow(CWE-122) exist in DHCP client function of VxWorks on MELSEC-Q Series C Controller Module.

■Impact

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

■Countermeasures

We have fixed the vulnerability at the following version.

Module Name	Version
Q12DCCPU-V	First 5 digits of serial number are “24032” or later.

■Mitigations/Workarounds

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

- Disable the DHCP function in "Security Settings" of the C language controller settings/monitor tool if the product is in "Extended mode " and the DHCP client function is not required.
- Update DHCP server to the latest version.
- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a trusted LAN that is properly divided by routers and firewalls.

■Contact information

Please contact your local Mitsubishi Electric representative.

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