Denial-of-Service Vulnerability in
Ethernet Communication Extension Unit (GC-ENET-COM) of GOC35 Series

Release date: March 31, 2023

Last update date: March 31, 2023

Mitsubishi Electric India Pvt. Ltd.

Overview

Mitsubishi Electric India is aware of a Denial-of-Service (DoS) vulnerability in Ethernet communication Extension unit (GC-ENET-COM) of GOC35 series due to signal handler race condition (*CWE-364*). If a malicious attacker sends specially crafted packets, communication error may occur and then may result in a Denial-of-Service (DoS) condition. (*CVE-2023-1285*)

CVSS

CVE-2023-1285 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H, Base Score:7.5.

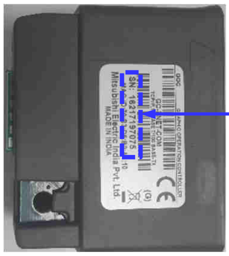
Affected products

Extension unit GC-ENET-COM fixed in the COM 1 slot of all versions of GOC 35 Main unit..

Affected product version is as shown below.

No.	Unit	Model Name	Serial Number
1	COM Extension unit	GC-ENET-COM	**16**XXXXXXXXX (First 2 digits of 11-digit serial number of unit are “16” and indicate product version)

Refer to serial number label on the left side of Extension unit GC-ENET-COM as shown below.



Serial number is shown as
SN: **16**XXXXXXXXX

Description

When Extension unit GC-ENET-COM is configured as Modbus TCP Sever and receives a large number of specially crafted packets from an attacker to any UDP port, it will not be able to process Modbus communication due to signal handler race condition (*CWE-364*) that occurs between Interrupt Service routine and processing code of extension unit, so falls into Denial-of-Service (DoS) condition.

Communication resumes only if the power of the Main unit is switched off and on or hot swapping of Extension unit GC-ENET-COM from Main unit.

Impact

A malicious attacker may cause a Denial-of-Service (DoS) of Modbus TCP communication.

Countermeasures

Firmware of Extension unit GC-ENET-COM which first 2 digits of 11-digit serial number of unit are “**17**” has been fixed.

Firmware update in Extension unit GC-ENET-COM is possible at factory only. Please contact your local Mitsubishi Electric India representative.

Mitigations

Mitsubishi Electric India recommends that customer should take the following mitigations to minimize the risk of exploiting this vulnerability if the mentioned countermeasures cannot be implemented.

1. Use a firewall, virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.
2. Locate control system networks and remote devices behind firewalls and isolate them from the business network to restrict access from untrusted networks and hosts.
3. Restrict physical access to your computer and network equipment on the same network.

Acknowledgement

Mitsubishi Electric India would like to thank Faruk Kazi and Parul Sindhwad from COE-CNDS lab, VJTI, Mumbai, India, who reported the vulnerability.

Contact information

Please contact your local Mitsubishi Electric India representative.

Update history

March 31, 2023.

First release.