Denial-of-Service Vulnerability in MELSOFT Transmission Port (TCP/IP)

Release date: May 27, 2021
Mitsubishi Electric Corporation

■Overview

Denial-of-Service (DoS) vulnerability exists in MELSOFT transmission port (TCP/IP) of MELSEC iQ-R series CPU modules due to improper session management. An attacker can cause resource exhaustion and DoS condition on a target by not closing a connection properly. (CVE-2021-20591)

The product models and firmware versions affected by this vulnerability are listed below.

■CVSS

CVE-2021-20591 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score:5.3

■Affected products

The following modules are affected:

Model name	Firmware Version
R00/01/02CPU	all versions
R04/08/16/32/120(EN)CPU	all versions
R08/16/32/120SFCPU	all versions
R08/16/32/120PCPU	all versions
R08/16/32/120PSFCPU	all versions

■Description

A denial-of-service (DoS) vulnerability exists in MELSOFT transmission port (TCP/IP) of MELSEC iQ-R series CPU modules due to Uncontrolled Resource Consumption (CWE-400).

■Impact

If a malicious attacker does not close the connection to the MELSOFT transmission port (TCP/IP), legitimate clients will not be able to connect to the MELSOFT transmission port (TCP/IP).

・If multiple MELSOFT transmission ports (TCP/IP) are open, the other ports are not affected.
・Sequence control is not affected.

■Countermeasures

Please carry out the mitigations/workarounds below.

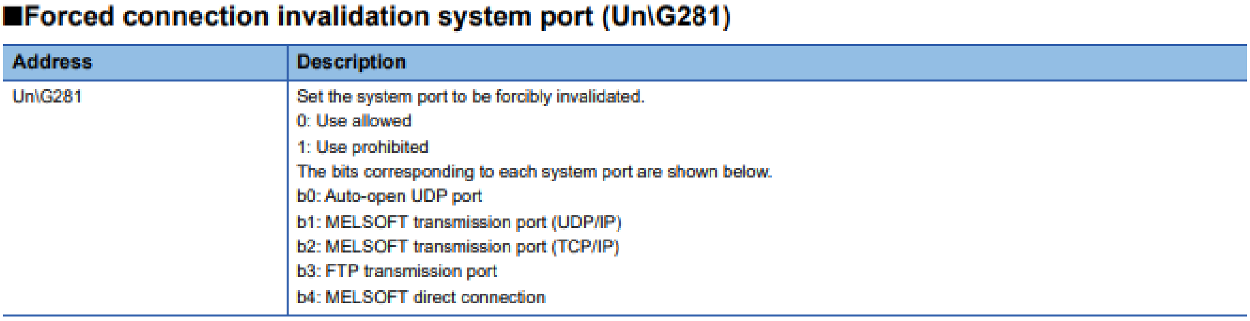
If this vulnerability is expoited, legitimate user can recover by disabling the port with the forced connection invalidation function and re-enabling the port.

For example, excerpt from the manual※1 and how to set the MELSEC iQ-R series CPU module are shown below.

※1：MELSEC iQ-R Ethernet User’s Manual (Application) Appendix 3 Buffer Memory

＜Example＞

・Excerpt from the manual



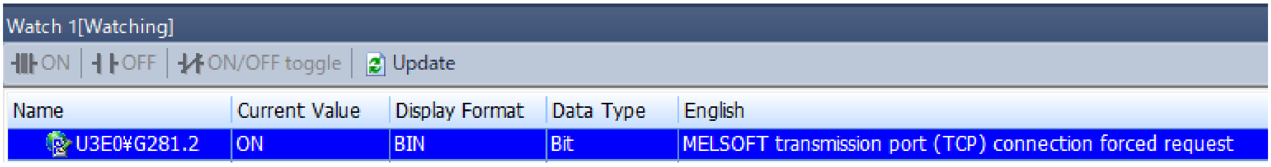
■Forced connection invalidation system port (Un\G281)

Address	Description
Un\G281	Set the system port to be forcibly invalidated. 0: Use allowed 1: Use prohibited The bits corresponding to each system port are shown below. b0: Auto-open UDP port b1: MELSOFT transmission port (UDP/IP) b2: MELSOFT transmission port (TCP/IP) b3: FTP transmission port b4: MELSOFT direct connection

・Setting method

Set b2 to “ON” on the watch or Device/Buffer Memory Batch Monitor. After that, by setting b2 to “OFF”, legitimate clients can connect.

＜Example：Watch＞



Name	Current Value	Display Format	Data Type	English
U3E0¥G281.2	ON	BIN	Bit	MELSOFT transmission port (TCP) connection forced request

■Mitigations/Workarounds

< Mitigations >

Mitsubishi Electric recommends that customers take either or a combination of 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.
- Use the IP filter function※2 to restrict the connectable IP addresses.
- Use the MELSOFT transmission port (UDP/IP).

※2：MELSEC iQ-R Ethernet User's Manual(Application) 1.13 Security "IP filter"

< Workarounds >

If port 5007 of the MELSOFT transmission port (TCP/IP) is not used, set b2 to "1" in advance with the forced connection invalidation function described in the Conutermeasures.

■Acknowledgement

Mitsubishi Electric would like to thank Younes Dragoni of Nozomi Networks who reported this vulnerability.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

https://www.mitsubishielectric.com/fa/support/index.html