Multiple Denial of Service (DoS) Vulnerabilities in TCP/IP Protocol Stack of MELSEC Series Remote I/O

Release date: December 16, 2021
Last update date: April 18, 2024
Mitsubishi Electric Corporation

Overview

Multiple Denial of Service (DoS) vulnerabilities due to Improper Input Validation (CWE-20[1]) exist in TCP/IP protocol stack on MELSEC Series Remote I/O. A remote attacker may cause a DoS condition in MELSEC Series Remote I/O by sending specially crafted packets. (CVE-2020-35683, CVE-2020-35684, CVE-2021-31401)

CVSS[2]

CVE-2020-35683 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
CVE-2020-35684 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
CVE-2021-31401 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

Affected products and versions are below.

MELSEC Series Remote I/O(*)

Product Name	Version
NZ2FT-EIP	All versions
NZ2FT-MT	
NZ2FT-PN	
NZ2FT-GN	
NZ2FT-PBV	
NZ2FT-BT	

(*) These products are sold in limited regions.

Description

Multiple DoS vulnerabilities due to Improper Input Validation (CWE-20) exist in TCP/IP protocol stack on MELSEC Series Remote I/O. (CVE-2020-35683, CVE-2020-35684, CVE-2021-31401)

Impact

A remote attacker may cause a DoS condition in MELSEC Series Remote I/O by sending specially crafted packets.

Countermeasures for Customers

There are no plans to release a fixed version. Customers using the affected products may take measures through mitigations and workarounds.

Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of these vulnerabilities:
- Use a router, firewall, virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use these products within a LAN and block access from untrusted networks and hosts through firewalls.
- Restrict physical access to affected products and any network devices on the network to which the products are connected. (e.g. storing in locked cabinets, attaching seals to unused Ethernet/USB ports)

Contact information

Please contact your local Mitsubishi Electric representative.

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

1 https://cwe.mitre.org/data/definitions/20.html
2 https://www.first.org/cvss/v3.1/specification-document

Update history

April 18, 2024

Changed the description of countermeasures.