Denial-of-Service Vulnerability in TCP/IP Stack of Embedded Ethernet

Release date: November 26, 2020
FANUC Corporation

■Outline

There is a denial-of-service vulnerability in TCP/IP stack of Embedded Ethernet on FANUC CNC. If this vulnerability is exploited by malicious attackers, the network functions of the products may stop. If you are using a product that is affected by this vulnerability, please take measures such as workarounds.

■Description

The vulnerability found this time is shown below.

CVE-ID	Reference URL
CVE-2020-12739	https://nvd.nist.gov/vuln/detail/CVE-2020-12739

■Impact

If this vulnerability is exploited by malicious attackers, the network functions of the products may stop.

■Affected products

Following series of Embedded Ethernet

- FANUC Series 30i/31i/32i-B Plus, 30i/31i/32i/35i-B
- FANUC Series 0i-F Plus, 0i-F
- FANUC Power Motion i-A
- FANUC Series 30i/31i/32i-A
- FANUC Series 0i-D, 0i-C, 0i-B
- FANUC Series 16i/18i/21i/20i-B

■Countermeasures and mitigation / workarounds

Please consider the following two measures.

If a phenomenon occurs, it can be recovered by turning the power off / on.

- Countermeasure 1

  Please identify unauthorized communication devices and take measures to prevent unauthorized attacks.

- Countermeasure 2

  Please restrict unauthorized access from the outside by installing a firewall or the like.

We recommend that you take appropriate security measures for the entire system.

■Reference Information

- Japan Vulnerability Notes “JVN#84959128FANUC i Series CNC vulnerable to denial-of-service (DoS)”
  https://jvn.jp/en/jp/JVN84959128/index.html