Multiple Vulnerabilities in TCP/IP Stack

Release date: November 26, 2020
FANUC Corporation

■Outline

There are multiple vulnerabilities in TCP/IP stack of FANUC CNC. If these vulnerabilities are exploited by malicious attackers, the CNC system or the network functions of the products may stop. If you are using a product that is affected by these vulnerabilities, please take measures such as workarounds.

■Description

The vulnerabilities found this time are shown below.

CVE-ID	Reference URL
CVE-2019-12264	https://nvd.nist.gov/vuln/detail/CVE-2019-12264
CVE-2020-11901	https://nvd.nist.gov/vuln/detail/CVE-2020-11901
CVE-2020-11903	https://nvd.nist.gov/vuln/detail/CVE-2020-11903
CVE-2020-11907	https://nvd.nist.gov/vuln/detail/CVE-2020-11907
CVE-2020-11910	https://nvd.nist.gov/vuln/detail/CVE-2020-11910
CVE-2020-11911	https://nvd.nist.gov/vuln/detail/CVE-2020-11911
CVE-2020-11912	https://nvd.nist.gov/vuln/detail/CVE-2020-11912
CVE-2020-11914	https://nvd.nist.gov/vuln/detail/CVE-2020-11914

■Impact

If these vulnerabilities are exploited by malicious attackers, the CNC system or the network functions of the products may stop.

■Affected products

Following series of Embedded Ethernet and Fast 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

- CERT/CC Vulnerability Note “VU#257161 Treck IP stacks contain multiple vulnerabilities”
  https://www.kb.cert.org/vuls/id/257161
- ICS Advisory “ICSA-20-168-01 Treck TCP/IP Stack”
  https://www.us-cert.gov/ics/advisories/icsa-20-168-01
- JSOF “Ripple20”
  https://www.jsof-tech.com/ripple20/
- Treck Inc. “Vulnerability Response Information”
  https://treck.com/vulnerability-response-information/