Vulnerabilities in FANUC Robot Controllers

Version 02
Issued Date : March 18, 2022
FANUC CORPORATION

Version	Date	Description
01	2021/12/16	The first edition registration
02	2022/03/18	Updated the description of Overview

■Overview

Two vulnerabilities have been reported for FANUC Robot Controllers. If these vulnerabilities are exploited by malicious attackers, the system software may stop working correctly due to data corruption. The vulnerabilities do not expose controller information. If you are using a product that is affected by these vulnerabilities, please take measures such as the workarounds described below.

■Description

The reported vulnerabilities are shown below.

CVE-ID	Reference URL
CVE-2021-32996	https://nvd.nist.gov/vuln/detail/CVE-2021-32996
CVE-2021-32998	https://nvd.nist.gov/vuln/detail/CVE-2021-32998

■Impact

If these vulnerabilities are exploited by malicious attackers, the system software of the products listed in “Affected products” may stop working correctly.

■Affected products

The following series of FANUC Robot Controllers are affected.

- FANUC Robot series R-30iA controller
- FANUC Robot series R-30iA Mate controller
- FANUC Robot series R-30iB controller
- FANUC Robot series R-30iB Mate controller
- FANUC Robot series R-30iB Plus controller
- FANUC Robot series R-30iB Mate Plus controller
- FANUC Robot series R-30iB Compact Plus controller
- FANUC Robot series R-30iB Mini Plus Controller

■Countermeasures

Please consider the following four countermeasures. If the system software is stopped and cannot be recovered, please contact us.

- Countermeasure 1
  Please restrict unauthorized access by using FANUC Server Access Control (FSAC).
- Countermeasure 2
  For customers using software version V9.30 or later, please restrict communication protocols available by setting the network access protocol level in the network setting section of the iHMI guide screen.
- Countermeasure 3
  Please identify unauthorized communication devices and take precautions to prevent unauthorized attacks.
- Countermeasure 4
  Please restrict unauthorized access by using devices that include a firewall or VPN.

We recommend that you take appropriate security measures for the entire system, not limited to the vulnerabilities described above.

■Reference information

- Industrial Control System | CISA – US-CERT “ICS Advisory (ICSA-21-243-02) FANUC Robot Controllers”
  https://us-cert.cisa.gov/ics/advisories/icsa-21-243-02