ロボット制御装置における脆弱性について

第 2 版

発行日 2022 年 3 月 18 日

ファナック株式会社

版数	年月日	改版内容
01	2021/12/16	初版登録
02	2022/03/18	概要の記載内容を更新

■概要

当社製ロボット制御装置において、2 つの脆弱性があることが判明しました。これらの脆弱性を悪意のある攻撃者に悪用された場合、データの破損により、システムの停止等の影響を受ける可能性があります。これらの脆弱性により、制御装置の情報が流出することはありません。

本脆弱性の影響を受ける商品をご使用の場合は、以下に記されている対策の実施をお願い致します。

■脆弱性の説明

今回判明した脆弱性を以下に示します。

CVE 識別番号	参照サイト
CVE-2021-32996	https://nvd.nist.gov/vuln/detail/CVE-2021-32996
CVE-2021-32998	https://nvd.nist.gov/vuln/detail/CVE-2021-32998

■脆弱性がもたらす脅威

悪意のある攻撃者に脆弱性を悪用された場合、システムの停止等の影響を受ける可能性があります。

■影響を受ける商品

当社下記シリーズのロボット制御装置が、影響を受けます。

- 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

■対策方法

以下の 4 つの対策をご検討ください。

なお、システムが停止してしまい、復旧できなくなった場合には当社へご連絡ください。

- 対策 1

  ロボット制御装置のファナックサーバーアクセス制御(FSAC)を設定し、外部からの不正なアクセスを制限してください。

- 対策 2
  ロボットソフトウェアのバージョンが V9.30 もしくはそれ以降の場合は、初期設定ガイドのネットワーク設定でアクセスレベルを上げることで、通信可能なプロトコルを制限してください。
- 対策 3
  不正な通信機器を特定し、不正な攻撃を行わないように対策してください。
- 対策 4
  ファイアウォール/VPN 機能搭載のデバイスを設置し、外部からの不正なアクセスを制限してください。

今回確認された脆弱性に限らず、システム全体において適切なセキュリティ対策を講じて頂くことを推奨致します。

■参考情報

- Japan Vulnerability Notes「JVNVU#93757182 FANUC 製ロボットコントローラにおける複数の脆弱性」
  https://jvn.jp/vu/JVNVU93757182/index.html