TCP/IP スタックにおける複数の脆弱性について

公開日 2020 年 11 月 26 日

ファナック株式会社

■概要

当社製 CNC で使用されている TCP/IP スタックおいて複数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、ネットワークの停止やシステムの停止等の影響を受ける恐れがあります。本脆弱性の影響を受ける製品をご使用の場合は、回避策等の対策の実施をお願い致します。

■脆弱性の説明

今回判明しました脆弱性を以下に示します。

CVE 識別番号	参照サイト
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

■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、ネットワークの停止やシステムの停止等の影響を受ける可能性があります。

■影響を受ける製品

当社下記シリーズの組込みイーサネットおよびファストイーサネット

- 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

■対策方法及び軽減策・回避策

以下の 2 つの対策をご検討ください。

なお、現象が発生した場合には、電源の OFF/ON で復旧することができます。

- 対策 1

  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 2
  ファイアウォールなどの設置により、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いたします。

■参考情報

- Japan Vulnerability Notes「JVNVU#94736763 Treck 製 IP スタックに複数の脆弱性」
  https://jvn.jp/vu/JVNVU94736763/index.html
- 図研エルミック株式会社「KASAGO 製品における脆弱性に関するお知らせ」
  https://www.elwsc.co.jp/news/4136/