MTTT261501
2022 年 6 月 21 日
株式会社ジェイテクト

TOYOPUC 製品における認証の欠如による PLC 機能停止の脆弱性について

1. 概要

TOYOPUC 製品において、重要な機能に対する認証の欠如により PLC 機能が停止する脆弱性の存在が判明しました。

CVSS V3 における基本値は 7.7 となります。
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H/E:P/RL:W/RC:C/CR:L/IR:L/AR:M/MAV:L/MAC:H/MPR:H/MUI:N/MS:U/MC:L/MI:H/MA:H

【参考】
CVSS（共通脆弱性評価システム）については、以下 URL をご参照ください。
https://www.ipa.go.jp/security/vuln/CVSSv3.html

2. 影響を受ける製品

本内容の影響を受ける製品は、以下となります。

製品名称	型式	対象バージョン
PC10G-CPU	TCC-6353	全て
PC10GE	TCC-6464	全て
PC10P	TCC-6372	全て
PC10P-DP	TCC-6726	全て
PC10P-DP-IO	TCC-6752	全て
PC10B-P	TCC-6373	全て
PC10B	TCC-1021	全て
PC10E	TCC-4737	全て
PC10EL	TCC-4747	全て
Plus CPU	TCC-6740	全て
PC3JX	TCC-6901	全て
PC3JX-D	TCC-6902	全て
PC10PE	TCC-1101	全て
PC10PE-1616P	TCC-1102	全て
PCDL	TKC-6688	全て
Nano 10GX	TUC-1157	全て
Nano CPU	TUC-6941	全て

3. 想定される影響
遠隔の第三者により、PLC の停止、通信の停止など任意の操作を実行される可能性があります。

4. 対策
【軽減策】
次の回避策のいずれか、または組み合わせを適用することで本脆弱性の影響を軽減できます。

・当該システムのネットワークをファイアウォール等で業務ネットワークから分離して運用する。
・外部からのアクセスが必要な場合は、VPN 等の安全な方法でアクセスする。VPN はバージョンアップを実施し、常に最新の状態にしておく。
・制御システム機器のネットワークへの接続を最小限にし、特定端末のみ接続できるように IP フィルタ機能を使用し、インターネットには直接接続しない。
・LAN ポートロックを使用して、HUB の空きポートに不正な機器が接続できないようにする。

5. 更新履歴
2022/6/21　　本脆弱性情報を公開しました。

6. お問い合わせ先
本内容に関するお問い合わせにつきましては、以下 URL までお願いします。
https://ma.jtekt.co.jp/form/vulnerability

以上