MTTT181701
2021 年 9 月 1 日
株式会社ジェイテクト

TOYOPUC 製品のイーサネット機能におけるサービス拒否（DoS）の脆弱性について

1. 概要

TOYOPUC 製品のイーサネット機能にサービス拒否（DoS）脆弱性の存在が判明しました。悪意のある第三者によって送信された大量のパケットを受信することで、該当通信ポートが DoS 状態となる可能性があります。

CVSS V3 における基本値は 4.3、となります。
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

【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
PC10B-E/C	TCU-6521	全て
PC10E	TCC-4737	全て
Plus CPU	TCC-6740	全て
Plus EX	TCU-6741	全て
Plus EX2	TCU-6858	全て
PC10PE	TCC-1101	全て
PC10PE-1616P	TCC-1102	全て
EF10	TCU-6982	全て
Plus EFR	TCU-6743	全て
Plus EFR2	TCU-6859	全て
Plus 2P-EFR	TCU-6929	全て
Plus BUS-EX	TCU-6900	全て
FL/ET-T-V2H	THU-6289	全て
2PORT-EFR	THU-6404	全て
Nano 10GX	TUC-1157	全て
Nano CPU	TUC-6941	全て
Nano 2ET	TUU-6949	全て
Nano Safety	TUC-1085	全て
Nano Safety RS00IP	TUU-1086	全て
Nano Safety RS01IP	TUU-1087	全て

3. 想定される影響
この攻撃を受けている間、正常なクライアントが通信ポートに接続できなくなる可能性があります。

本脆弱性は、PLC のシーケンス制御に影響はありません。
サービス運用妨害(DoS)の状態が終了すれば通信は正常状態に戻ります。
この脆弱性で該当イーサネットポートの通信以外の機能が影響を受けることはありません。

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、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
2021/9/2　　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