MTTT111901
2021 年 4 月 15 日
株式会社ジェイテクト

外部機関からの TOYOPUC 製品におけるイーサネット通信への脆弱性指摘について

1. 概要

TOYOPUC 製品のイーサネット通信に関しての外部機関からの指摘の内容と対処方法についてご案内いたします。
内容をご確認いただき、必要に応じて対処の実施をお願いいたします。

2. 指摘の内容

悪意の第三者によって TOYOPUC 製品のイーサネット通信のコネクションをオープンしたままにされた場合、リンクパラメータの設定によっては、本来の通信相手とイーサネット通信ができなくなる。

3. 影響のある製品

本内容の影響を受ける製品は、以下の製品にてリンクパラメータ「イーサネット」または「イーサネット(32 ポート)」の設定を行い、「相手不特定パッシブ」として利用している場合となります。

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
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

4. 詳細な指摘内容
TOYOPUC 製品のイーサネット通信において、下記の場合に該当のコネクションとのイーサネット通信を確立できなくなります。
・コネクション切断時に、正常にコネクションをクローズしなかった場合
・コネクションを接続した状態で放置している場合
復旧には PLC のリセットスタートまたは電源再投入が必要です。

CVSS V3 における基本値は 7.5、現状値は 7.2 となります。
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C

【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

5. 本内容がもたらす脅威
TOYOPUC 製品のイーサネット通信のコネクションが悪意の第三者より正常にクローズされない場合、該当のコネクションにおいて本来の通信相手機器とのイーサネット通信が確立できなくなります。

6. 対処方法
本内容の影響を軽減したい場合は、以下の「軽減策」をご参照の上、設定変更の実施をお願いします。
また、本内容に関わらず、製品が接続されるネットワークに不審な機器が接続されないよう、ファイアウォール等の適切なセキュリティ設定とネットワーク管理を行うことを推奨いたします。

【軽減策】
リンクパラメータ「イーサネット」または「イーサネット(32 ポート)」の詳細設定の各種タイマの設定より、無受信タイマを「設定する」に設定してください。
リンクパラメータ設定後は、**パソコンと PLC を USB ケーブルで接続**し、パラメータの書込みを行ってください。
書込み完了後は、リセットスタートまたは電源再投入を行ってください。
リセットスタートまたは、電源再投入でパラメータ変更が有効になります。

無受信タイマが有効になることで、正常にクローズされなかったコネクションを設定時間経過後にリセットすることができ、該当のコネクションが通信可能な状態となります。
設定内容詳細につきましては、各機器の取扱説明書をご参照ください。

7. 更新履歴
2021/4/15　　情報を公開しました。

8. 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、以下メールアドレスまでお願いします。
JJP_PSIRT@jtekt.co.jp

以上