

外部機関からの TOYOPUC FL-net 機能の脆弱性指摘について

1. 概要

TOYOPUC 製品の FL-net 機能に脆弱性が存在することが判明いたしました。

その内容および対応方法についてご案内いたします。

内容をご確認いただき、必要に応じて軽減策またはセキュリティ強化の適用をお願いします。

2. 脆弱性詳細

TOYOPUC 製品の FL-net 通信において、メッセージ通信機能に起因した攻撃によりサービス運用妨害の脆弱性が存在します。

攻撃者によって意図的に細工されたメッセージフレームを受信すると PLC のプログラム実行が停止する可能性があります。

CVSS V3 における基本値は 6.5、現状値は 5.9 となります。

CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A: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>

3. 脆弱性がもたらす脅威

悪意を持った第三者が工場内に侵入し 且つ FL-net ネットワークに不正に接続し TOYOPUC へ上記攻撃を行うと PLC のプログラム実行が停止する可能性があります。

復旧には電源再投入、または PLC のリセットスタートが必要となります。

※信頼された FL-net 製品で独立したネットワークを構築している場合は、影響はありません。

4. 影響を受ける製品

製品名称	型式	脆弱性対象バージョン	セキュリティ強化バージョン
PC10G-CPU	TCC-6353	3.91 未満	3.91 以上
2PORT-EFR	THU-6404	1.50 未満	1.50 以上
Plus CPU	TCC-6740	3.11 未満*1	3.11 以上*1
Plus EX	TCU-6741	バージョンなし*1	
Plus EX2	TCU-6858	バージョンなし*1	
Plus EFR	TCU-6743	バージョンなし*1	
Plus EFR2	TCU-6859	バージョンなし*1	
Plus 2P-EFR	TCU-6929	バージョンなし*1	
PC10P-DP	TCC-6726	1.50 未満	1.50 以上
PC10P-DP-IO	TCC-6752	1.50 未満	1.50 以上
Plus BUS-EX	TCU-6900	2.13 未満*1	2.13 以上*1
Nano 10GX	TUC-1157	3.00 未満	3.00 以上
Nano 2ET	TUU-6949	2.40 未満	2.40 以上
PC10PE	TCC-1101	1.02 未満	1.02 以上
PC10PE-1616P	TCC-1102	1.02 未満	1.02 以上
PC10E	TCC-4737	1.12 未満	1.12 以上
FL/ET-T-V2H	THU-6289	F2.8 E1.5 未満	F2.8 E1.5 以上
PC10B	TCC-1021	1.11 未満	1.11 以上
PC10B-P	TCC-6373	1.11 未満	1.11 以上
Nano CPU	TUC-6941	2.08 未満	2.08 以上
PC10P	TCC-6372	1.05 未満	1.05 以上
PC10GE	TCC-6464	1.04 未満	1.04 以上

<表 1>

*1: Plus シリーズの拡張ボードはバージョンアップ不要です。

Plus シリーズの拡張ボードをお使いの場合、拡張ボードを装着している Plus CPU または Plus BUS-EX をバージョンアップしてください。

5. 軽減策とセキュリティ強化

1) 軽減策

FL-net ネットワークに不審な機器が接続されないようネットワークを適切に管理してください。

他のイーサネット機器やインターネット環境からアクセスがされないよう FL-net 製品で構築したネットワークにしてください。

2) セキュリティ強化

上記のような攻撃手段に対して製品のセキュリティ強化を実施しました。

セキュリティ強化をご希望されるお客様は、セキュリティ強化バージョン(表1)のご使用をご検討ください。ご使用中の製品のバージョンアップも承ります。

・製品のバージョンは以下のいずれかの方法で確認できます。

1) 製品前面等に貼付されているバージョンシールを確認する。

2) PLC のレジスタの値を確認する。確認するレジスタにつきましては、各製品取扱説明書をご参照ください。

6. 更新履歴

2021/06/29 本脆弱性情報を公開しました。

7. 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://form.k3r.jp/jtektmt/inquiry7>

以上