MTTT162802E
June 30, 2021
JTEKT CORPORATION

Vulnerability of FL-net function in TOYOPUC products pointed out by an external organization

1. Introduction

A vulnerability was found in the FL-net function of TOYOPUC products.
We will inform you of the contents and how to deal with it.
Please check the contents and apply mitigation measures and security enhancements as necessary.

2. Details of the vulnerability

In the FL-net communication of TOYOPUC products, a vulnerability of denial-of-service exists due to an attack caused by the message communication function.
When the affected TOYOPUC product receives a message frame intentionally changed by an attacker, the program execution of the PLC may stop.

The CVSS V3.0 base score is 6.5.
The CVSS V3.0 temporal score is 5.9.
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

[Reference]
Please refer to the following URL about CVSS score.
https://www.first.org/cvss/

3. Threats posed by vulnerabilities

If a third party with malicious intent invades the factory and illegally connects to the FL-net network and carries out the above attack on TOYOPUC, the program execution of the PLC may stop.
To recover, you need to power cycle or reset the PLC.
* There is no problem if you establish an independent network using a highly reliable FL-net product.

4. Affected products

Affected product	Type	Vulnerable version	Enhanced security version
PC10G-CPU	TCC-6353	3.91 Less than	3.91 or later
2PORT-EFR	THU-6404	1.50 Less than	1.50 or later
Plus CPU	TCC-6740	3.11 Less than *1	3.11 or later *1
Plus EX	TCU-6741	No version*1	
Plus EX2	TCU-6858	No version*1	
Plus EFR	TCU-6743	No version*1	
Plus EFR2	TCU-6859	No version*1	
Plus 2P-EFR	TCU-6929	No version*1	
PC10P-DP	TCC-6726	1.50 Less than	1.50 or later
PC10P-DP-IO	TCC-6752	1.50 Less than	1.50 or later
Plus BUS-EX	TCU-6900	2.13 Less than *1	2.13 or later *1
Nano 10GX	TUC-1157	3.00 Less than	3.00 or later
Nano 2ET	TUU-6949	2.40 Less than	2.40 or later
PC10PE	TCC-1101	1.02 Less than	1.02 or later
PC10PE-1616P	TCC-1102	1.02 Less than	1.02 or later
PC10E	TCC-4737	1.12 Less than	1.12 or later
FL/ET-T-V2H	THU-6289	F2.8 E1.5 Less than	F2.8 E1.5 or later
PC10B	TCC-1021	1.11 Less than	1.11 or later
PC10B-P	TCC-6373	1.11 Less than	1.11 or later
Nano CPU	TUC-6941	2.08 Less than	2.08 or later
PC10P	TCC-6372	1.05 Less than	1.05 or later
PC10GE	TCC-6464	1.04 Less than	1.04 or later

＜table 1＞

*1: There is no need to update the Plus Series expansion board.
If you are using a Plus Series expansion board, please update a Plus CPU or a Plus BUS-EX to which the expansion board is connected.

5. Mitigation and security enhancement

1）Mitigation measures

Manage the network properly so that suspicious devices are not connected to the FL-net network.
Use a network established with FL-net products so that it is not accessed by other Ethernet devices or the Internet environment.

2）Enhanced security

Enhanced product security against the above attack methods.

Customers who wish to enhance security should consider using the enhanced security version (Table 1).
We also accept version updates for the products you are using.
-You can check the product version by one of the following methods.

1) Check the version seal on the front of the product.
2) Check the PLC register value. For the register to check, refer to the instruction manual of each product.

6. History

June 29, 2021　This information has been released.

7. Contact us

For inquiries regarding this content, please contact the following URL.
https://ma.jtekt.co.jp/form/vulnerabilitye