MTTT111901
April 15th, 2021
JTEKT CORPORATION

Vulnerability of Ethernet communication in TOYOPUC products pointed out by an external organization

1. Introduction

We will inform you of a content pointed out to us by an external organization regarding and how to deal with it on this document.

Please check contents and implement workaround measures as necessary.

2. Content pointed out

If Ethernet communication of the affected product is left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.

3. Affected products

The following products are affected by this vulnerability when a link parameter is set to “Ethernet” or “Ethernet (32ports)” and used as "TCP Destination Non-Specified Passive Open".

Affected product	Type	Affected version
PC10G-CPU	TCC-6353	All
PC10GE	TCC-6464	All
PC10P	TCC-6372	All
PC10P-DP	TCC-6726	All
PC10P-DP-IO	TCC-6752	All
PC10B-P	TCC-6373	All
PC10B	TCC-1021	All
PC10B-E/C	TCU-6521	All
PC10E	TCC-4737	All
Plus CPU	TCC-6740	All
Plus EX	TCU-6741	All
Plus EX2	TCU-6858	All
Plus EFR	TCU-6743	All
Plus EFR2	TCU-6859	All
Plus 2P-EFR	TCU-6929	All
Plus BUS-EX	TCU-6900	All
FL/ET-T-V2H	THU-6289	All
2PORT-EFR	THU-6404	All

4. Detail content pointed out

In Ethernet communication of TOYOPUC products, Ethernet communication cannot be established with a device that should be connected in the following cases.

-If a connection is not closed correctly when the connection is disconnected

-If a connection is connected and left in that state

Reset/start or power-on of the PLC is required for recovery.

The CVSS V3.0 base score is 7.5.
The CVSS V3.0 temporal score is 7.2.
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

“Reference”

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

5. Threat by this pointed out content

When a connection is not closed correctly by an attacker in Ethernet communication of TOYOPUC products, after that, Ethernet communication cannot be established with a device that should be connected.

6. Workarounds and mitigations

If you want to mitigate a threat, please refer to the following "Workaround" to change settings.

Regardless of this matter, we recommend that you make appropriate security settings such as firewalls and manage a network to prevent suspicious devices from connecting to the network to which a product is connected.

“Workaround”

Please set “Non-Reception timer” to "Enable" from in various timer settings of a detailed setting of a link parameter "Ethernet" or "Ethernet (32Port)".

After setting the link parameter, **please connect a computer and a PLC with a USB cable** and write the link parameter.
After writing is completed, perform a reset/start or power-on again.
After reset/start or power-on, the parameter changes take effect.

When Non-Reception timer is enabled, the connection that was not closed correctly can be reset after the set time has elapsed. And a connection can communicate with a device that should be connected.
For details on the settings, refer to the User's Manual of each device.

7. History

April 15th, 2021 This information has been released.

8. Contact us

For inquiries regarding this content, please contact the following e-mail address.

E-mail: JJP_PSIRT@jtekt.co.jp