MTTT181701E
Sept 1st, 2021
JTEKT CORPORATION

Denial of service (DoS) vulnerability in Ethernet function of TOYOPUC products

1. Introduction

A denial of service (DoS) vulnerability has been found in Ethernet function of TOYOPUC products. When the relevant TOYOPUC products receives many packets sent by a malicious third party, the relevant communication port on the TOYOPUC products may enter a DoS state.

The CVSS V3.0 base score is 4.3.
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

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

2. Affected products

The products affected by this vulnerability are as follows.

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
PC10PE	TCC-1101	All
PC10PE-1616P	TCC-1102	All
EF10	TCU-6982	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
Nano 10GX	TUC-1157	All
Nano CPU	TUC-6941	All
Nano 2ET	TUU-6949	All
Nano Safety	TUC-1085	All
Nano Safety RS00IP	TUU-1086	All
Nano Safety RS01IP	TUU-1087	All

3. Expected impact

During this attack, a normal client may not be able to connect to the communication port.

PLC sequence control is not affected by this vulnerability.
If the Denial of Service (DoS) condition has ended, communication will return to normal state.
This vulnerability does not affect any function other than communication of the relevant Ethernet port.

4. Mitigations

"Workaround"

You can mitigate the impact of this vulnerability by applying one or more of the following workarounds.

- Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- When remote access is required, use secure methods, such as virtual private networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices
- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.
- To prevent unauthorized devices from being connected to the free ports of the HUB, use LAN port lock to close the free ports.

5. History

Sept 2nd, 2021: This information has been released.

6. Contact us

For inquiries regarding this content, please contact the following URL.
https://form.k3r.jp/jtektmt/inquiry7e