MTTT261501
June 21, 2022
JTEKT CORPORATION

About a vulnerability of PLCs to stop by the lack of authentication capabilities on TOYOPUC products

1. Introduction

TOYOPUC products have a vulnerability of PLCs stop by the lack of authentication capabilities for important operations.

The CVSS V3.0 base score is 7.7.
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H/E:P/RL:W/RC:C/CR:L/IR:L/AR:M/MAV:L/MAC:H/MPR:H/MUI:N/MS:U/MC:L/MI:H/MA:H

[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
PC10E	TCC-4737	All
PC10EL	TCC-4747	All
Plus CPU	TCC-6740	All
PC3JX	TCC-6901	All
PC3JX-D	TCC-6902	All
PC10PE	TCC-1101	All
PC10PE-1616P	TCC-1102	All
PCDL	TKC-6688	All
Nano 10GX	TUC-1157	All
Nano CPU	TUC-6941	All

3. Expected impact

This vulnerability allows an attacker to remotely stop a PLC or stop communication.

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, use IP filter functions to allow only specific personal computer/device to connect, 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

June 21, 2022: This information has been released.

6. Contact us

For inquiries regarding this content, please contact the following URL.

https://form.k3r.jp/jtektmt/inquiry7e