# CVE Detail – CVE-2022-29951

JTEKT TOYOPUC PLCs through 2022-04-29 mishandle authentication. They utilize the CMPLink/TCP protocol (configurable on ports 1024-65534 on either TCP or UDP) for a wide variety of engineering purposes such as starting and stopping the PLC, downloading and uploading projects, and changing configuration settings. This protocol does not have any authentication features, allowing any attacker capable of communicating with the port in question to invoke (a subset of) desired functionality.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.22328

## CVSS Scoring

CVSS v3.1 Score: 9.1

Severity: CRITICAL

## Mapped CWE(s)

* CWE-306: Missing Authentication for Critical Function

## CAPEC(s)

* CAPEC-12: Choosing Message Identifier
* CAPEC-166: Force the System to Reset Values
* CAPEC-216: Communication Channel Manipulation
* CAPEC-36: Using Unpublished Interfaces or Functionality
* CAPEC-62: Cross Site Request Forgery

## Affected Products

* cpe:2.3:o:jtekt:pc10g-cpu\_tcc-6353\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10ge\_tcc-6464\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10p\_tcc-6372\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10p-dp\_tcc-6726\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10p-dp-io\_tcc-6752\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10b-p\_tcc-6373\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10b\_tcc-1021\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10e\_tcc-4737\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10el\_tcc-4747\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:plus\_cpu\_tcc-6740\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc3jx\_tcc-6901\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc3jx-d\_tcc-6902\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10pe\_tcc-1101\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pc10pe-1616p\_tcc-1102\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:pcdl\_tkc-6688\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:nano\_10gx\_tuc-1157\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:jtekt:nano\_cpu\_tuc-6941\_firmware:-:\*:\*:\*:\*:\*:\*:\*