# CVE Detail – CVE-2022-29952

Bently Nevada condition monitoring equipment through 2022-04-29 mishandles authentication. It utilizes the TDI command and data protocols (60005/TCP, 60007/TCP) for communications between the monitoring controller and System 1 and/or Bently Nevada Monitor Configuration (BNMC) software. These protocols provide configuration management and historical data related functionality. Neither protocol has any authentication features, allowing any attacker capable of communicating with the ports in question to invoke (a subset of) desired functionality.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.17204

## 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* CAPEC-36: Using Unpublished Interfaces or Functionality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:bakerhughes:bently\_nevada\_3701\/40\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:bakerhughes:bently\_nevada\_3701\/44\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:bakerhughes:bently\_nevada\_3701\/46\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:bakerhughes:bently\_nevada\_60m100\_firmware:-:\*:\*:\*:\*:\*:\*:\*