# CVE Detail – CVE-2019-9201

Multiple Phoenix Contact devices allow remote attackers to establish TCP sessions to port 1962 and obtain sensitive information or make changes, as demonstrated by using the Create Backup feature to traverse all directories.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.82925

## CVSS Scoring

CVSS v3.1 Score: 9.8

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* CAPEC-36: Using Unpublished Interfaces or Functionality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:phoenixcontact:ilc\_131\_eth\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:phoenixcontact:ilc\_131\_eth\/xc\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:phoenixcontact:ilc\_151\_eth\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:phoenixcontact:ilc\_151\_eth\/xc\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:phoenixcontact:ilc\_171\_eth\_2tx\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:phoenixcontact:ilc\_191\_eth\_2tx\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:phoenixcontact:ilc\_191\_me\/an\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:phoenixcontact:axc\_1050\_firmware:-:\*:\*:\*:\*:\*:\*:\*