# CVE Detail – CVE-2022-30276

The Motorola MOSCAD and ACE line of RTUs through 2022-05-02 omit an authentication requirement. They feature IP Gateway modules which allow for interfacing between Motorola Data Link Communication (MDLC) networks (potentially over a variety of serial, RF and/or Ethernet links) and TCP/IP networks. Communication with RTUs behind the gateway is done by means of the proprietary IPGW protocol (5001/TCP). 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: 0.29887

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## 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* CAPEC-36: Using Unpublished Interfaces or Functionality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:motorola:moscad\_ip\_gateway\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:motorola:ace\_ip\_gateway\_\(4600\)\_firmware:\*:\*:\*:\*:\*:\*:\*:\*