# CVE Detail – CVE-2022-30313

Honeywell Experion PKS Safety Manager through 2022-05-06 has Missing Authentication for a Critical Function. According to FSCT-2022-0051, there is a Honeywell Experion PKS Safety Manager multiple proprietary protocols with unauthenticated functionality issue. The affected components are characterized as: Honeywell Experion TCP (51000/TCP), Safety Builder (51010/TCP). The potential impact is: Manipulate controller state, Manipulate controller configuration, Manipulate controller logic, Manipulate controller files, Manipulate IO. The Honeywell Experion PKS Distributed Control System (DCS) Safety Manager utilizes several proprietary protocols for a wide variety of functionality, including process data acquisition, controller steering and configuration management. These protocols include: Experion TCP (51000/TCP) and Safety Builder (51010/TCP). None of these protocols have any authentication features, allowing any attacker capable of communicating with the ports in question to invoke (a subset of) desired functionality. There is no authentication functionality on the protocols in question. An attacker capable of invoking the protocols' functionalities could achieve a wide range of adverse impacts, including (but not limited to), the following: for Experion TCP (51000/TCP): Issue IO manipulation commands, Issue file read/write commands; and for Safety Builder (51010/TCP): Issue controller start/stop commands, Issue logic download/upload commands, Issue file read commands, Issue system time change commands. A mitigating factor with regards to some, but not all, of the above functionality is that these require the Safety Manager physical keyswitch to be in the right position.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.35258

## 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* CAPEC-36: Using Unpublished Interfaces or Functionality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:honeywell:safety\_manager\_firmware:-:\*:\*:\*:\*:\*:\*:\*