# CVE Detail – CVE-2022-30317

Honeywell Experion LX through 2022-05-06 has Missing Authentication for a Critical Function. According to FSCT-2022-0055, there is a Honeywell Experion LX Control Data Access (CDA) EpicMo protocol with unauthenticated functionality issue. The affected components are characterized as: Honeywell Control Data Access (CDA) EpicMo (55565/TCP). The potential impact is: Firmware manipulation, Denial of service. The Honeywell Experion LX Distributed Control System (DCS) utilizes the Control Data Access (CDA) EpicMo protocol (55565/TCP) for device diagnostics and maintenance purposes. This protocol does not 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 protocol in question. An attacker capable of invoking the protocols' functionalities could issue firmware download commands potentially allowing for firmware manipulation and reboot devices causing denial of service.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.30152

## 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* CAPEC-36: Using Unpublished Interfaces or Functionality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:honeywell:experion\_lx\_firmware:\*:\*:\*:\*:\*:\*:\*:\*