# CVE Detail – CVE-2022-30314

Honeywell Experion PKS Safety Manager 5.02 uses Hard-coded Credentials. According to FSCT-2022-0052, there is a Honeywell Experion PKS Safety Manager hardcoded credentials issue. The affected components are characterized as: POLO bootloader. The potential impact is: Manipulate firmware. The Honeywell Experion PKS Safety Manager utilizes the DCOM-232/485 serial interface for firmware management purposes. When booting, the Safety Manager exposes the Enea POLO bootloader via this interface. Access to the boot configuration is controlled by means of credentials hardcoded in the Safety Manager firmware. The credentials for the bootloader are hardcoded in the firmware. An attacker with access to the serial interface (either through physical access, a compromised EWS or an exposed serial-to-ethernet gateway) can utilize these credentials to control the boot process and manipulate the unauthenticated firmware image (see FSCT-2022-0054).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.13889

## CVSS Scoring

CVSS v3.1 Score: 4.6

Severity: MEDIUM

## Mapped CWE(s)

* CWE-798: Use of Hard-coded Credentials

## CAPEC(s)

* CAPEC-191: Read Sensitive Constants Within an Executable
* CAPEC-70: Try Common or Default Usernames and Passwords

## ATT&CK Techniques

* T1078.001: Default Accounts
* T1552.001: Credentials In Files

## Used By (Actors/Tools)

* TrickBot (malware)
* Stuxnet (malware)
* Smoke Loader (malware)
* HyperStack (malware)
* Emotet (malware)
* Hildegard (malware)
* BlackEnergy (malware)
* XTunnel (malware)
* pngdowner (malware)
* StrelaStealer (malware)
* Pysa (malware)
* Agent Tesla (malware)
* jRAT (malware)
* Azorult (malware)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* LaZagne (tool)
* Pupy (tool)
* QuasarRAT (tool)
* Indrik Spider (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* TA505 (intrusion-set)
* Ember Bear (intrusion-set)
* TeamTNT (intrusion-set)
* Leafminer (intrusion-set)
* Magic Hound (intrusion-set)
* MuddyWater (intrusion-set)
* Kimsuky (intrusion-set)
* FIN13 (intrusion-set)
* Scattered Spider (intrusion-set)
* RedCurl (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* APT3 (intrusion-set)
* HomeLand Justice (campaign)
* APT33 (intrusion-set)

## Affected Products

* cpe:2.3:o:honeywell:safety\_manager\_firmware:\*:\*:\*:\*:\*:\*:\*:\*