# CVE Detail – CVE-2022-30312

The Trend Controls IC protocol through 2022-05-06 allows Cleartext Transmission of Sensitive Information. According to FSCT-2022-0050, there is a Trend Controls Inter-Controller (IC) protocol cleartext transmission of credentials issue. The affected components are characterized as: Inter-Controller (IC) protocol (57612/UDP). The potential impact is: Compromise of credentials. Several Trend Controls building automation controllers utilize the Inter-Controller (IC) protocol in for information exchange and automation purposes. This protocol offers authentication in the form of a 4-digit PIN in order to protect access to sensitive operations like strategy uploads and downloads as well as optional 0-30 character username and password protection for web page access protection. Both the PIN and usernames and passwords are transmitted in cleartext, allowing an attacker with passive interception capabilities to obtain these credentials. Credentials are transmitted in cleartext. An attacker who obtains Trend IC credentials can carry out sensitive engineering actions such as manipulating controller strategy or configuration settings. If the credentials in question are (re)used for other applications, their compromise could potentially facilitate lateral movement.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.03843

## CVSS Scoring

CVSS v3.1 Score: 6.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-319: Cleartext Transmission of Sensitive Information

## CAPEC(s)

* CAPEC-102: Session Sidejacking
* CAPEC-117: Interception
* CAPEC-383: Harvesting Information via API Event Monitoring
* CAPEC-477: Signature Spoofing by Mixing Signed and Unsigned Content
* CAPEC-65: Sniff Application Code

## ATT&CK Techniques

* T1040: Network Sniffing
* T1056.004: Credential API Hooking

## Used By (Actors/Tools)

* TrickBot (malware)
* cd00r (malware)
* JumbledPath (malware)
* RDFSNIFFER (malware)
* NOKKI (malware)
* VersaMem (malware)
* Ursnif (malware)
* Zeus Panda (malware)
* J-magic (malware)
* Emotet (malware)
* Regin (malware)
* Line Dancer (malware)
* FoggyWeb (malware)
* MESSAGETAP (malware)
* Zebrocy (malware)
* FinFisher (malware)
* Carberp (malware)
* ZxShell (malware)
* Penquin (malware)
* Impacket (tool)
* Empire (tool)
* PoshC2 (tool)
* Responder (tool)
* NBTscan (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Sandworm Team (intrusion-set)
* APT28 (intrusion-set)
* Kimsuky (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* DarkVishnya (intrusion-set)
* PLATINUM (intrusion-set)
* Salt Typhoon (intrusion-set)
* APT33 (intrusion-set)

## Affected Products

* cpe:2.3:o:honeywell:trend\_iq412\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:honeywell:trend\_iq411\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:honeywell:trend\_iq422\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:honeywell:trend\_iq4nc\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:honeywell:trend\_iq4e\_firmware:\*:\*:\*:\*:\*:\*:\*:\*