# CVE Detail – CVE-2022-29960

Emerson OpenBSI through 2022-04-29 uses weak cryptography. It is an engineering environment for the ControlWave and Bristol Babcock line of RTUs. DES with hardcoded cryptographic keys is used for protection of certain system credentials, engineering files, and sensitive utilities.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.23721

## CVSS Scoring

CVSS v3.1 Score: 5.5

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:a:emerson:openbsi:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:emerson:openbsi:5.9:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:emerson:openbsi:5.9:sp1:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:emerson:openbsi:5.9:sp2:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:emerson:openbsi:5.9:sp3:\*:\*:\*:\*:\*:\*