# CVE Detail – CVE-2017-3225

Das U-Boot is a device bootloader that can read its configuration from an AES encrypted file. For devices utilizing this environment encryption mode, U-Boot's use of a zero initialization vector may allow attacks against the underlying cryptographic implementation and allow an attacker to decrypt the data. Das U-Boot's AES-CBC encryption feature uses a zero (0) initialization vector. This allows an attacker to perform dictionary attacks on encrypted data produced by Das U-Boot to learn information about the encrypted data.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.15405

## CVSS Scoring

CVSS v3.0 Score: 4.6

Severity: MEDIUM

## Mapped CWE(s)

* CWE-329: Generation of Predictable IV with CBC Mode

## Affected Products

* cpe:2.3:a:denx:u-boot:\*:\*:\*:\*:\*:\*:\*:\*