# CWE Detail – CWE-329

## Description

The product generates and uses a predictable initialization Vector (IV) with Cipher Block Chaining (CBC) Mode, which causes algorithms to be susceptible to dictionary attacks when they are encrypted under the same key.

## Extended Description

CBC mode eliminates a weakness of Electronic Code
 Book (ECB) mode by allowing identical plaintext blocks to
 be encrypted to different ciphertext blocks. This is
 possible by the XOR-ing of an IV with the initial plaintext
 block so that every plaintext block in the chain is XOR'd
 with a different value before encryption. If IVs are
 reused, then identical plaintexts would be encrypted to
 identical ciphertexts. However, even if IVs are not
 identical but are predictable, then they still break the
 security of CBC mode against Chosen Plaintext Attacks
 (CPA).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2020-5408: encryption functionality in an authentication framework uses a fixed null IV with CBC mode, allowing attackers to decrypt traffic in applications that use this functionality

**•** CVE-2017-17704: messages for a door-unlocking product use a fixed IV in CBC mode, which is the same after each restart

**•** CVE-2017-11133: application uses AES in CBC mode, but the pseudo-random secret and IV are generated using math.random, which is not cryptographically strong.

**•** CVE-2007-3528: Blowfish-CBC implementation constructs an IV where each byte is calculated modulo 8 instead of modulo 256, resulting in less than 12 bits for the effective IV length, and less than 4096 possible IV values.

**•** CVE-2011-3389: BEAST attack in SSL 3.0 / TLS 1.0. In CBC mode, chained initialization vectors are non-random, allowing decryption of HTTPS traffic using a chosen plaintext attack.

## Modes of Introduction

**•** Implementation: Developers might dismiss the importance of an unpredictable IV and choose an easier implementation to save effort, weakening the scheme in the process.

## Common Consequences

**•** Impact: Read Application Data — Notes: If the IV is not properly initialized, data that is encrypted can be compromised and leak information.

## Potential Mitigations

**•** Implementation: NIST recommends two methods of generating unpredictable IVs for CBC mode [REF-1172]. The first is to generate the IV randomly. The second method is to encrypt a nonce with the same key and cipher to be used to encrypt the plaintext. In this case the nonce must be unique but can be predictable, since the block cipher will act as a pseudo random permutation. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** In both of these examples, the initialization vector (IV) is always a block of zeros. This makes the resulting cipher text much more predictable and susceptible to a dictionary attack.

## Notes

**•** Maintenance: As of CWE 4.5, terminology related to randomness, entropy, and
 predictability can vary widely. Within the developer and other
 communities, "randomness" is used heavily. However, within
 cryptography, "entropy" is distinct, typically implied as a
 measurement. There are no commonly-used definitions, even within
 standards documents and cryptography papers. Future versions of
 CWE will attempt to define these terms and, if necessary,
 distinguish between them in ways that are appropriate for
 different communities but do not reduce the usability of CWE for
 mapping, understanding, or other scenarios.