1.1.1 CBC Mod ile Rastgele IV Kullanılmaması (Not Using a Random IV with CBC Mode) (CWE-329)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Hassas Bilgilere Yetkisiz Erişim, Gizlilik İhlali

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Uygulamalar tahmin edilebilir "CBC Mod için IV (Initilization Vector)" değeri kullandıklarında bu durum güvenlik riski oluşturur. Örneğin oturum id'lerinin tahmin edilebilmesi ve saldırganın oturumu ele geçirip birisi adına işlemler yürütmesi gibi veya hangi amaç için IV kullanılıyorsa o amaçta gizliliğinin ihlal edilmesi gibi. CBC mod için IV'ler **statik tanımlandıklarında** "CBC Mod ile Rastgele IV Kullanılmaması" açıklığı olarak işaretlenirler. Uygulamalardaki bu açıklığa şu şekilde bir örnek verilebilir:

Java:

```
// Güvensiz Kod Parçası

// ENG: Use of Static IV in an Encryption
// TR : Şifrelemede Statik IV Kullanılması

IvParameterSpec ivParams = new IvParameterSpec(CONST_IV);
```

Burada IV değerini alma görevini yapan IvParameterSpec() metodu statik (sabit) bir IV değeri almaktadır. IV'nin statik (sabit) olması kodu güvensiz kılan unsurdur. Bu güvensiz kod parçasının güvenli şekle dönüşmüş hali şu şekildedir:

Java:

```
// Güvenli Kod Parçası

// ENG: Use of Cryptographically Secure PRNG IV in an Encryption
// TR : Şifrelemede Kriptografik Olarak Güvenli PRNG IV Kullanılması

SecureRandom random = new SecureRandom();
byte[] iv = new byte[cipher.getBlockSize()];
random.nextBytes(iv);                    // iv nesnesine SecureRandom ile
                                         // rastgele byte değer atanır.
IvParameterSpec ivParams = new IvParameterSpec(iv);
```

Burada ilk olarak SecureRandom ile güvenli rastgele değer üreteci nesnesi tanımlanmaktadır. Ardından iv için bir byte nesne tanımlanmaktadır. Daha sonra bu iv nesnesine SecureRandom ile rastgele bir byte değer atanmaktadır. Son olarak sabit (statik) değer içermeyen, rastgele değer içeren IV nesnesi IV parametresini alma görevi yapan IvParameterSpec() metoduna verilmektedir. Böylece güvenli ve rastgele IV değeri kullanarak kod güvenli hale geçmektedir.

Kurum uygulamada IV'nin güvenli rastgele değer üreteçleriyle değil, statik tanımlandığı tespit edilmiştir:

::::::: BULGU :::::::

Açıklığın Önlemi:

CBC Mod'da tahmin edilebilir IV açıklığını kapamak için IV nesnesi güvenli rastgele değer üreteçleri ile rastgele oluşturulmalıdır. Statik tanımlanmamalıdır.

Referanslar:

1. https://cwe.mitre.org/data/definitions/329.html
2. https://www.geeksforgeeks.org/random-nextbytes-method-in-java-with-examples/
3.