1.1.1 Yakalanmamış İstisna (Improper Exception Handling) (CWE-248)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Uygulamanın çökmesi, hassas verilerin ifşası, diğer beklenmedik davranışlar

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Uygulamalarda zaman zaman uygulamaların normal akışını bozan istisnalar (exception'lar) meydana gelebilmektedir. Örneğin veritabanı, dosya erişimi gibi bazı işlemlerde istisnalar fırlayabilmektedir. Bu işlemlerde olası istisnalar yakalanacak şekilde kodlama yapılmazsa uygulamada beklenmeyen davranışlar gerçekleşebilir. Örneğin çökme, bilgi ifşası gibi. Bir saldırgan yakalanmamakta olan bir istisnayı tetikleyerek uygulamanın servis dışı kalmasını sağlayabilir veya hata durumuna göre farklı aksiyonlar alabilir.

Yakalanmamış İstisna açıklığını somutlaştırmak için şu örnek verilebilir:

Java - Güvensiz Hal:

```
public static void loadLib() {

      // Eğer LIB_NAME mevcut değilse
      // yakalanmayan bir istisna fır-
      // layacaktır.

    System.loadLibrary(LIB_NAME);
}
```

Java - Güvenli Hal:

```
// Handle All Possible Exceptions within the Error-Prone Method

public static void loadLib() {
    try {

        System.loadLibrary(LIB_NAME);

    }
    catch (SecurityException se) {

        // SecurityException Yakalama

    }
    catch (UnsatisfiedLinkError sle) {

        // UnsatisfiedLinkError Yakalama

    }

}
```

Java - Güvenli Hal (2):

```
// Aggregate Potential Exceptions to Calling Code

public static void loadLib() throws UnsatisfiedLinkError, SecurityException {

   System.loadLibrary(LIB_NAME);

}
```

Görüldüğü gibi ilk örnekte istisna fırlatabilir bir işlem try-catch ile çevrelenmemiştir. Bu güvensiz kodlamadır. İkinci örnekte istisna fırlatabilir bir işlem try-catch ile çevrelenmiştir. Bu güvenli kodlamadır. Üçüncü örnekte istisna fırlatabilir bir işlem ilgili metodun fırlatılabilir istisnalar listesi tanımı ile hata yönetimi kapsamına alınmıştır. Bu da alternatif bir güvenli kodlamadır.

Kurum uygulamasında istisna fırlatabilen işlemlerin istisnalarını yakalayacak bir kodlamada bulunulmadığı tespit edilmiştir:

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

Açıklığın Önlemi:

İstisna fırlamasına neden olabilecek herhangi bir metot try-catch blok'ları ile sarmalanmalıdır ve;

- Beklenen olası istisnalar açıkça (explicitly) yakalanmalıdır.
- Beklenmeyen istisnalar ise açıkça (explicitly) varsayılan (default) bir tanım ile yakalama kapsamına dahil edilmelidir.

Referanslar:

1. https://cwe.mitre.org/data/definitions/248.html
2.