1.1.1 Güvenli Olmayan Dizi Tanımlaması (Array Declared Public, Final and Static) (CWE-582)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Güvenlik riski doğması

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Uygulamalarda dizi nesneleri / değişkenleri public, final ve static tanımlanabilmektedir. final kullanımı umulduğu üzere dizinin modifiye edilmesini önler ama dizinin elemanlarının modifiye edilmesini önlemek için yeterli değildir. final belirteci nesneye / değişkene bir dizinin sadece bir defa atanmasını zorlar, ancak dizi elemanlarına değerlerin yalnızca bir kez atanabilmesini garanti etmez. Böylesi bir durumda bir de dizi public tanımlanırsa zararlı bir program dizinin depolu değerlerini değiştirebilir.

Bu problemi göstermek adına örnek java kod bloklarına yer verilmiştir:

Java - Güvensiz Kod Bloğu:

```
public class example {
    /**
    * Get a new random id.
    */

    public static final String[] ALLOWED_URLS = new String[]
{"http://amazon.com", "http://cnn.com"};

    public String getRandId() {
        Random random = new SecureRandom();
        byte[] randomBytes = new byte[csrfSize];
        random.nextBytes(randomBytes);
        return Hex.encodeHexString(randomBytes);
    }
}
```

Java - Güvenli Kod Bloğu:

```java
public class example {
    public static void main(String[] argv)
        throws Exception
    {
        try {

            // creating object of ArrayList<Character>
            List<Character> list = new ArrayList<Character>();

            // populate the list
            list.add('X');
            list.add('Y');

            // printing the list
            System.out.println("Initial list: " + list);

            // getting unmodifiable list
            // using unmodifiableList() method
            List<Character> immutablelist = Collections
.unmodifiableList(list);

            // Adding element to new Collection
            System.out.println("\nTrying to modify" + " the
unmodifiablelist");
            immutablelist.add('Z');
        }

        catch (UnsupportedOperationException e) {
            System.out.println("Exception thrown : " + e);
        }
    }
}
```

Java güvensiz kod bloğunda bir dizi nesnesinin hataen public, final ve static tanımlandığı gösterilmiştir. Bu güvensiz kullanımdır. Çünkü final kullanımında umulanın aksine dizinin elemanları değiştirilebilirdir.

Java güvenli kod bloğunda ise bir dizi nesnesi güvenli bir şekilde - ArrayList ile - tanımlanmıştır. Ardından Collection ile unmodifiableList() kullanarak dizinin elemanları değiştirilemez yapılmıştır. Bu sayede diziye önce X ve Y değerleri eleman olarak eklenebilirken dizi elemanları değiştirilemez yapıldığında Z değeri diziye eleman olarak eklenemez duruma gelmiştir.

Çoğu durumda bir diziyi public, final ve static tanımlamak beklenmeyen durumlara yol açabilir. Gelecekte beklenmeyen güvenlik riskleri doğurabilir. Yaşanabilecek olası

problemlerin önüne şimdiden geçmek için bu güvensiz tanımlamanın düzeltilmesi önerilmektedir. Bu açıklığa Güvenli Olmayan Dizi Tanımlaması (CWE-582) açıklığı adı verilir.

Kurum uygulamada Güvenli Olmayan Dizi Tanımlaması (CWE-582) açıklığı tespit edilmiştir.

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

Açıklığın Önlemi:

- Dizi (field'ının / instance variable'ının) erişebilirliği azaltılmalıdır - örneğin private yapılmalıdır - veya dizi üyesinin tipi değiştirilemez tip yapılmalıdır.
- Dizi için uygun bir collection tipi kullanılmalıdır. Collection kullanarak kullanıcı dizi elemanı güncellemelerinin izinli olup olmadığını kontrol edebilir. Kullanıcı Collections.unmodifiableList() kullanarak collection'ın güncellenmesini önleyebilir. Ayrıca Collection değiştirilemez olsa bile collection'da depolu tip'lerin de değiştirilemez olduğundan emin olunmalıdır. Aksi takdirde sabit varsayılan elemanlar üzerinde istenmeyen değişiklikler yine görülecektir.

Referanslar:

1. https://cwe.mitre.org/data/definitions/582.html
2. https://vulncat.fortify.com/en/detail?category=Unsafe%20Mobile%20Code&subcategory=Unsafe%20Array%20Declaration#Java%2fJSP