1.1.1 Public Bir Metottan Private Dizi Döndürülmesi (Private Array Returned From A Public Method) (CWE-495)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Dizi içeriğinin kapsam dışından modifiye edilebilmesi

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Class'larda (sınıflarda) dizi veri tipli instance variable'lar (diğer adıyla field'lar, Türkçesiyle sınıf değişkenleri) değişebilir nesnelerdir. Yani bu türden nesneler üzerine yazma yapılabilir. Eğer uygulama public metot üzerinden bir private dizi field'ı referansı dönüyorsa bu dönen referansa yapılacak herhangi bir modifkasyon private field'ı etkileyecektir.

Bir public metottan private dizi türündeki field'ın referansını döndürmek bu private field'a herhangi bir yerden modifikasyon yapılmasına izin verir. Böylesi bir modifikasyon esnekliği uygulamanın akış kontrolünü etkileyebilir, veri sızıntısına yol açabilir, istemeden private dizi değişkeni üzerine veri yazmaya izin verebilir. Public bir metotta private dizi referansı döndürülürse "Public Bir Metottan Private Dizi Döndürülmesi (CWE-495)" açıklığı olarak ele alınırlar.

Örneğin bu açıklığa sahip Java ve C++ kod blokları verilmiştir:

Java - Güvensiz Kod Bloğu:

```java
// Returns A Reference To A Private Array Type Field

public class Person {

   private final String name;
   private String[] visited = {"New York", "California", "Colorado"};

   public String[] getVisited() {
      return visited;
   }
}
```

Bu örnekte gösterildiği üzere private bir dizi değişkeni referansı public bir metotta döndürülmektedir. Bu durum güvensiz kabul edilmektedir.

Java - Güvenli Kod Bloğu:

```
// Returns A Reference To A “Cloned” Array Type Field,
// Not Affecting Object's Field

public class Person {

   private final String name;
   private String[] visited = {"New York", "California", "Colorado"};

   public String[] getVisited() {
     return visited.clone();
  }
}
```

Bu örnekte ise private dizi değişkeni public metotta döndürülmemektedir, onun yerine private dizi değişkeninin klonu public metotta döndürülmektedir. Bu ise private dizi değişkeninin orijinalini modifiye edilmemiş tutatacağından güvenli kodlama örneği olarak yer almaktadır.

C++ - Güvensiz Kod Bloğu:

```
// Returns A Reference To A “Cloned” Array Type Field,
// Not Affecting Object's Field

class Color {

   private:

      int[2] colorArray;
      int colorValue;

   public:

      Color () : colorArray { 1, 2 }, colorValue (3) { };

      // Private Dizi Referansı Döndürür
      int[2] & fa () { return colorArray; }

      // Private Int Referansı Döndürür
      int & fv () { return colorValue; }

};

int main () {

   Color color;

   // (!) Private Dizi Elemanını Modifiye Eder
   color.fa () [1] = 42;

   // (!) Private Int’i Modifiye Eder
   color.fv () = 42;

   return 0;
}
```

Bu örnekte ise 2 elemanlı private int dizisi colorArray, bir de private int değişkeni colorValue tanımlanmıştır. fa() ve fv() isimli tanımlanan public metotlar ise colorArray ve colorValue private değişkenlerin referansını döndürmektedir. Bu durum main() içerisinde fa() ve fv()’nin döndürdüğü referanslar üzerinden private değişkenlere veri yazmaya (dizi değişkeninin birinci elemanına 42, int değişkenine ise 42 değeri yazmaya) imkan vermektedir. Bu durum güvensiz kabul edilmektedir.

Kurum uygulamada "Public Bir Metottan Private Dizi Döndürülmesi (CWE-495)" açıklığı tespit edilmiştir:

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

Açıklığın Önlemi:

- Public metotta referans olarak dizi veri tipli private field'ın klonunu döndürün ve private field'ın orijinalini modifiye edilmemiş tutun.
- Alternatif olarak; dizi veri tipli private field'ın nasıl modifiye edileceğini yöneten public bir setter metot tanımlayın.
- Alternatif olarak; public metodu private olarak tanımlayın.

Referanslar:

1. https://cwe.mitre.org/data/definitions/495.html
2. https://stackoverflow.com/questions/28648533/how-to-protect-private-field-in-class-with-getter-in-java
3.