

1.1.1 Private Diziye Atanmış Public Veri (Public Data Assigned to Private Array) (CWE-496)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Private dizinin dışarıdan modifiye edilebilmesi

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Nesne yönelimli programlamalarda private tanımlanmış bir sınıf field (üye) dizisi encapsulation prensibi gereği sadece aynı sınıfın kendi metotları üzerinden erişilebilir ve modifiye edilebilir. Ancak private dizi field'ına public bir setter metodu ile public bir dizi atanırsa encapsulation ihlal olur. Çünkü artık private dizi public diziyi tuttuğundan dışarıdan erişilebilir ve modifiye edilebilir hale gelir. Bu dahili verinin kontrolü kaybı çeşitli zafiyetlere kapı aralar. Örneğin veri bütünlüğü sorunları, dahili verilerin sızdırılması veya güvenlik mekanizmalarının atlatılabilmesi gibi. Private dizilere public veri atanmasına "Private Diziye Atanmış Public Veri (CWE-496)" açıklığı adı verilir.

Örneğin bu açıklığa sahip Java kod bloğu verilmiştir:

Java - Güvensiz Kod Bloğu:

```
// Setting The Private Data Member Value Directly

public class Person {

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

    public void setVisited(String[] visited){
        this.visited = visited;
    }

}
```

Bu örnekte setVisited() metodu public olarak kontrol edilebilen bir diziyi private üye değişkene atamıştır. Bu ise Java'da diziler mutable (değişebilir) olduklarından çağırıcı metoda private diziyi doğrudan modifiye etme izni vermiştir. Bu nedenle güvensizdir. Private bir dizi değişkenine setter metodu ile public bir veri atamadan sakınılması gerekir.

Java - Güvenli Kod Bloğu:

```
// Setting The Private Data Member Value
// Through An Intermediate Object

public class Person {

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

    public void setVisited(String[] visited){
        this.visited = Arrays.copyOf(visited, visited.length);
    }
}
```

Bu örnekte ise private dizi değişkeni public setter metodu ile bir public referansı doğrudan almamaktadır. Bunun yerine public referansın gösterdiği verinin kopyasını almaktadır. Bu katmanlı kullanım güvenli olan yol kabul edilmektedir.

Kurum uygulamada "Private Diziye Atanmış Public Veri (CWE-496)" açıklığı tespit edilmiştir:

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

Açıklığın Önlemi:

- Nesnelerin bir sınıfın private üye değişkenlerini modifiye etmesine izin vermeyin.
- Public nesneden değerleri private üye değişkene kopyalamak için ara bir klon nesne oluşturun.

Referanslar:

1. <http://cwe.mitre.org/data/definitions/496.html>
2. <https://stackoverflow.com/questions/16125616/are-string-arrays-mutable>