

1.1.1 Switch İfadesinde Default Durumun Olmaması (Missing Default Case in Switch Statement (CWE-478)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Güvenliğin sürdürülebilirliğinin azalması

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Programlama dillerinde switch ifadesi bir ifadeyi belirli sayıda duruma karşı eşleşme kıyaslamasına tabi tutma ve eşleşilen duruma dallanma, sonra da break komutu ile dallanmayı sonlandırma işlemini yapar. Eğer switch ifadelerinde default eşleşme durumu bulunmazsa bu durum “Switch İfadesinde Default Durumun Olmaması (CWE-478)” açıklığı olarak ele alınır.

Switch ifadelerinde default duruma yer verilmemesi planlanmamış çalışma akışına sebebiyet verebilir. Bu durum çoğunlukla istemci girdilerinin uygulama tarafından belirlendiği durumlarda yaşanan problemlerden bir tanesidir. Uygulama kullanıcılarına istemci girdilerini kendi koyduğunda gelecek girdilerin bunlardan bir tanesi olacağını varsayar. Switch ifadesi ise buna göre tasarlanır. Ancak girdi “istemci” girdisi olduğu için kullanıcı uygulamanın koyduğu değerleri kolaylıkla manipule edebilir ve geçersiz bir girdi gönderebilir. Bu durumda geçersiz girdi switch ifadesindeki kıyaslamaları komple atlamış olur ve switch ifadesi ne için kullanılıyorsa o anlamda suistimal edilebilir.

- Örneğin switch ifadelerinde gelen girdiye göre güvenlik fonksiyonları çalışıyorsa geçersiz girdi girildiğinde güvenlik fonksiyonları atlatılmış olur ve uygulama switch'i atladiğından normal akışına güvensiz devam eder.
- Örneğin switch ifadelerinde gelen girdiye göre bir hesaplama yapılıyorsa (misal olarak anket için gelen oylar toplanıyorsa) geçersiz girdi girildiğinde switch atlanarak sonrasında devam edileceği için anket istatistiki verilerinin hesaplamasında bozulma yaşanabilir ve arayüze anket sonuçları basılamaz hale gelebilir. Bu da bir işlevin crash olması (çökmesi) anlamına gelir ki bir işlevde veya komple serviste servis dışı kalma sonucu doğurabilir.
- v.b.

Switch ifadesi öncesi, switch ifadesinin kendisi ve switch ifadesi sonrası switch ifadesinde default durum olmadığında suistima edilebilir. Uygulama kodlamasında switch ifadesinde default duruma yer verilmesi gerekir. Bu bir “**defansif programlama**” örneğidir ve planlanmamış durumlarda uygulamanın güvende kalmasını sağlar.

Bu açıklığı göstermek adına java örneklerine yer verilmiştir:

Java

```
//Güvensiz Kod Örneği  
  
switch (param) {  
    case 0:  
        doSomething();  
        break;  
    case 1:  
        doSomethingElse();  
        break;  
}
```

Bu örnekte switch ifadesi default durum içermediğinden güvensizdir.

Java:

```
// Güvensiz Kod Örneği 2  
  
switch (param) {  
    default:  
        error();  
        break;  
    case 0:  
        doSomething();  
        break;  
    case 1:  
        doSomethingElse();  
        break;  
}
```

Bu örnekte ise default durum eşleşme durumları arasında en başta yer aldığından güvensizdir. Default durum eşleşme durumları arasında en sona yerleştirilmelidir.

Java:

```
// Güvenli Kod Örneği

switch (param) {
    case 0:
        doSomething();
        break;
    case 1:
        doSomethingElse();
        break;
    default:
        error();
        break;
}
```

Bu örnekte güvenli kullanım gösterilmiştir.

Not:

Bir istisna olarak bazı durumlarda switch ifadesinde olası tüm durumlar konulabilir ve switch ifadesine default durumu koymak gerekemeyebilir. Bu durumda default durumu koymama sadece switch ifadesinde “%100” kesinlikle başka eşleşme durumunun meydana gelmeyeceği belli olduğu zaman geçerli olur.

Kurum uygulamasında “Switch İfadesinde Default Durumun Olmaması” açıklığı tespit edilmiştir:

::::: BULGU :::::

Açıklığın Önlemi:

Kurum uygulamada kullanılan switch ifadelerine default eşleşme durumu ilave edilmelidir.

Referanslar:

1. <https://cwe.mitre.org/data/definitions/478.html>
2. <https://rules.sonarsource.com/java/RSPEC-131>
3. <https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Statements/switch>