

### 1.1.1 System.Exit() Kullanılması (Use of System Exit) (CWE-382)

**Açıklık Önem Derecesi:** Düşük

**Açıklığın Etkisi:** Servis Dışı Kalma

**Açıklığın Barındıran Dosyalar/Satırlar:**

Proje Dosyası/Dosya Adı	Satır Numarası

**Açıklığın Açıklaması:**

Java uygulamalardaki `java.lang.System.exit()` metodu Java Virtual Machine'i sonlandırarak mevcut programdan çıkış yapmayı sağlar. Bu metoda argüman olarak 0'dan farklı bir değer verilmesi genellikle anormal sonlandırmayı belirtmek için kullanılır. Java'daki bu metod C ve C++'daki `exit` komutuna benzerdir. Java'daki `System.Exit()`'in deklarasyonu şu şekildedir:

Java:

```
public static void exit(int status)
```

Aldığı değerler ise şu şekildedir:

Aldığı Değerler	Açıklaması
<code>exit(0)</code>	Genellikle başarılı sonlanmalar için kullanılır.
<code>exit(1)</code> veya <code>exit(-1)</code> veya sıfırdan farklı başka bir değer	Genellikle başarısız sonlanmalar için kullanılır.

Java dilinde `System.exit()`'in kullanıldığı güvensiz bir duruma örnek verilmiştir:

Java - Güvensiz Kod Bloğu:

```
Public void doPost(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {

    if (isAuthorized()) {

        try {
            updateDb(request);
        }
        catch (UpdateDbException ude)
        {
            logger.error("Caught Exception While Updating DB: " +
ude.toString());
            System.exit(1);
        }

        [..]
    }
}
```

J2EE uygulaması System.exit() kullandığında bu JVM'i kapatır. Bu kullanım bir web uygulama için asla iyi bir fikir değildir. Uygulamayı kapatabilen fonksiyona olası başarılı bir erişimde uygulama keyfi olarak servis dışı saldırganlarca bırakılabilir. Bu durum System.exit() Kullanılması (CWE-382) açıklığı olarak değerlendirilir.

Kurum uygulamada "System.exit() Kullanılması (CWE-382)" açıklığı tespit edilmiştir.

.....:BULGU:.....

### **Açıklığın Önlemi:**

Sonlandırma metodunun çağırılması kodu, arta kalan bir debug (hata ayıklama) kodundan dolayı yer alıyor olabilir veya koda eklenmiş J2EE olmayan üçüncü taraf bir uygulama kodundan dolayı yer alıyor olabilir. Bu kullanımlardan prod ortamda sakınılması gerekir.

Tavsiyeler genel manada şu şekildedir:

- Web uygulamalar System.exit() gibi virtual machine'in kapanmasına neden olan metotları çağdırmamalıdır.
- Web uygulama olmayan uygulamalar ise System.exit() içeren bir main() metodu belki kullanabilirler, fakat kodda main() dışında diğer konumlardan System.exit() genellikle çağdırmamalıdır.

### **Referanslar:**

1. <https://cwe.mitre.org/data/definitions/382.html>

2. <https://vulncat.fortify.com/en/detail?category=J2EE%20Bad%20Practices&subcategory=JVM%20Termination#Java%2fJSP>
3. <https://community.veracode.com/s/question/0D52T000051Yh4DSAS/cwe382-j2ee-bad-practices-use-of-systemexit>
4. <https://www.security-database.com/cwe.php?name=CWE-382>