1.1.1 Kısıtlanmamış Dosya Yükleme (Unrestricted File Upload) (CWE-434)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Servis Dışı Kalma

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Uygulamalarda kullanıcıların sınırsız boyutta dosya kaydetmesine izin verilmesi saldırganların dosya deposunu gereksiz/çöp dosyalarla doldurmasına veya dosya kaydetme işlemini yürüten işleyişi zorlayacak uzun yazma işlemleri gerçekleştirmelerine neden olabilir. Depolama alanının yorulması veya dosya alanının kullanılamayacak derecede kısıtlanması servis dışı bırakma sonucunu doğurabilir. Uygulama kodlarının kullanıcı tarafından depolama alanına yüklenen dosyaları kaydetmeden önce boyut kontrolü yapmaması ve potansiyel olarak herhangi bir boyutta dosya yüklenebilmesi "Kısıtlanmamış Dosya Yükleme" açıklığı olarak ele alınır.

Bu açıklığa örnek olarak Java kod bloğu verilmiştir:

Java - Güvensiz Kod Bloğu:

```
public void saveMultipartFile(CommonsMultipartFile multipartFile, String path)
throws IOException {

    FileOutputStream fos = new FileOutputStream(path);
    fos.write(multipartFile.getBytes());
    fos.close();

}
```

Bu örnekte alınan dosya içeriği herhangi bir boyut kontrolü yapılmadan diske yazdırılmaktadır.

Java - Güvenli Kod Bloğu:

```
public void saveMultipartFile(CommonsMultipartFile multipartFile, String path)
throws IOException {

    if (multipartFile.getSize() < MAX_SIZE) {
        FileOutputStream fos = new FileOutputStream(path);
        fos.write(multipartFile.getBytes());
        fos.close();
    }
    else {
        throw new IOException("Maximum file size exceeded!");
    }

}
```

Bu örnekte ise dosya içeriği boyut kontrolü sonrası diske yazdırılmaktadır.

Kurum uygulamada "Kısıtlanmamış Dosya Yükleme" açıklığı tespit edilmiştir:

:::: BULGU ::::

Açıklığın Önlemi:

- Saldırganların rastgele boyutlardaki dosyaları karşıya yüklemelerini önlemek için koda dosya boyutu kısıtı yerleştirin.
- İstemci taraflı yapılan boyut kontrollerine güvenmeyin.
- Bunun yerine dosyanın boyut kıyaslamasını tamamen sunucu taraflı uygulayın.
- Ayrıca sunucu taraflı boyut kontrolü yapılırken kullanıcılar tarafından sağlanan herhangi bir boyut parametresine de güvenmeyin.

Referanslar:

1. http://cwe.mitre.org/data/definitions/434.html
2. https://vulncat.fortify.com/en/detail?id=desc.content.html.often_misused_file_upload#Java%2fJSP