1.1.1 Şüpheli Yorumlar (Suspicious Comments) (CWE-546) (CWE-615)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Bilgi ifşası

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Uygulamada kaynak kodlar “bir hatanın (bug’ın) varlığını”, “tamamlanmamış bir fonksiyonun ifadesini” veya bir güvenlik zafiyetinin ifadesini içeren yorumlara sahip olabilmekteler. Örneğin; BUG, FIXME, HACK, TODO, LATER, LATER2 gibi ifadelerle yapılması icap eden iş yorum olarak not düşülebilmektedir. Bu türden yorumlar doğrudan olmasa da dolaylı yoldan güvenlik açıklığı oluşturmaktadırlar.

Örneğin bu açıklığın yer aldığı bir kod bloğuna şu şekilde örnek verilebilir:

Java:

```
// KÖTÜ KOD

if (user == null) {
    // TODO: Handle null user condition.
}
```

Bu örnekte tamamlanmamış bir fonksiyonun tamamlanmasına dönük öneride bulunan bir yorum yer almaktadır.

JSP:

```
// KÖTÜ KOD

<!--
      FIXME: 30 argümandan daha fazla çağırmak
             JDBC sunucusuna crash verdiriyor.
-->
```

Bu örnekte ise düzeltilmesi önerilen bir hatadan (bug'dan) bahseden bir yorum yer almaktadır. Bu v.b. yorumlar prod (canlı) ortamda yer alırsa prod (canlı) ortama başarılı sızma girişimlerinde saldırganlar tersine mühendislik ile (debugger araçları ile) bu v.b. string'leri elde edebilirler ve başarılı bir şekilde sızdıkları sunucuda belli bir mesafe katetmişken bu türden yorumlar sayesinde daha da fazla mesafe katedebililirler. Yani verebilecekleri zararın boyutunu bu v.b. yorumlardan yararlanarak arttırılabilirler. Bu nedenle bu v.b. yorumlar prod (canlı) ortamda yer almamalıdır.

Bahsedilen tarzdaki yorum satırları kötü kod kalitesine işaret ederler ve "Şüpheli Yorumlar (CWE-546)" açıklığı olarak ele alınırlar.

Kurum uygulamasında şüpheli yorumlar açıklığı tespit edilmiştir. Bu durum Şekil XXX. ABCDEF'de gösterilmiştir.

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

Açıklığın Önlemi:

Uygulamalar canlı (prod) ortama servis edilmeden (deploy edilmeden) önce bir hatanın (bug'ın) varlığını, tamamlanmamış bir fonksiyonu veya bir güvenlik zafiyetini konu edinen yorumlar kaynak kodlardan kaldırılmalıdır.

Referanslar:

1. https://cwe.mitre.org/data/definitions/546.html
2. https://cwe.mitre.org/data/definitions/615.html
3. https://www.zaproxy.org/docs/alerts/10027/
4.