1.1.1 SSL Doğrulama Atlatması (SSL Verification Bypass) (CWE-599)

Açıklık Önem Derecesi: Orta

Açıklığın Etkisi: Trafiğin izlenebilmesi

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Uygulamaların ve api'lerin haberleşmede https protokolü kullanması güvenli kabul edilir. Fakat https protokolü kullanılırken ssl/tls sertifika doğrulaması kontrolünün uygulanmaması güvensiz kabul edilir. Çünkü ssl/tls kullanıldığı ama sertifika doğrulamanın uygulanmadığı durumlarda saldırganlara istemciden sunucuya giden taleplerde araya girme, istemciye sahte sunucu sertifikası sağlama ve MITM (araya giren adam) saldırısı gerçekleştirme imkanı verilmiş olur. Saldırgan bu sayede istemcinin https trafiğindeki verileri okuyarak

- hassas verileri çalabilir,
- istemci tarafa gelen verileri manipüle ederek oltalama faaliyeti yürütebilir
- istemci tarafa gelen verileri yine manipüle ederek defacement (arayüz tahrifi) yapabilir
- istemci tarafa gelen verileri silerek dos etkisi oluşturabilir
- v.b.

Bu açıklığı göstermek adına örneklere yer verilmiştir:

Python - Güvensiz Kod Bloğu (1):

```
# Explicitly Disabling Ceritificate Validation in Requests

r = requests.get(REMOTE_SERVER_URL, verify=False)
```

Python - Güvensiz Kod Bloğu (2):

```
# Explicitly Disabling Ceritificate Validation in SSL
# Context for urllib and urllib2

ctx = ssl.create_default_context()
ctx.check_hostname = False
ctx.verify_mode = ssl.CERT_NONE
r = urlopen(REMOTE_SERVER_URL, context=ctx)
```

Python - Güvensiz Kod Bloğu (3):

```
# Explicitly Disabling Certificate Validation in urllib3

http = urllib3.PoolManager(cert_reqs='CERT_NONE')
r = http.request('GET', REMOTE_SERVER_URL)
```

Python güvensiz kod bloğu 1'de verify parametresi false olarak kullanılarak ssl sertifika doğrulama pasifleştirilmiştir. Python güvensiz kod bloğu 2'de ctx nesnesi hostname ve seritifka doğrulama adımı pasifleştirilmiştir. Python güvensiz kod bloğu 3'de cert_reqs parametresi CERT_NONE olarak kullanılarak ssl sertifika pasifleştirilmiştir. Tüm bu kullanımlar sakıncalıdır ve ssl doğrulama atlatma saldırılarının hedeflerindendir.

Kurum uygulamada SSL Doğrulama Atlatma (CWE-599) açıklığı tespit edilmiştir.

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

Açıklığın Önlemi:

Genel tavsiyeler şu şekildedir:

- Şifreli iletişimlerde gerek duyulan varlıkları sağlama noktasında tüm gerekli kontroller düzgünce uygulanmalıdır
- HTTPS işlevi sunan kütüphanelerin tüm parametreleri düzgünce yapılandırılmalıdır
- Seritifka doğrulama işlevi asla kapatılmamalıdır.

Referanslar:

1. https://cwe.mitre.org/data/definitions/599.html