

1.1.1 ATS Güvenliğinin Pasifleştirilmesi (App Transport Security Bypass) (CWE-319)

Açıklık Önem Derecesi: Yüksek

Açıklığın Etkisi: Hassas bilgilerin ele geçirilebilmesi

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

App Transport Security (ATS) iOS mobil uygulamalarda varsayılan olarak açık gelen, mobil uygulama ile back-end'i (arka ucu) veya mobil uygulama ile web servisleri arasında güvenli bağlantı kurmak için kullanılan bir best practice önlemidir. ATS, mobil uygulamaların back-end (arka uç) veya web servisler ile arasındaki iletişimin şifreli olması kısıtını koyar. Fakat geliştirici eliyle bu ayar pasifleştirilebilmektedir.

Objective-C veya Swift programlama dili ile yazılmış iOS uygulamalarda info.plist isimli konfigürasyon dosyasında NSAllowsArbitraryLoads anahtarının true yapılması mobil uygulama genelinde güvensiz bağlantılara (http bağlantılarına) tümüyle izin verir. Varsayılan olarak aktif gelen ATS güvenliğinin bu şekilde pasifleştirilmesi mobil uygulama ile back-end'i (arka ucu) veya web servisleri arasındaki trafiğin http üzerinden akmasına izin verir. Fakat bu durum MITM adı verilen saldırılara karşı mobil uygulama trafiğini riske sokar. Yani bu durum trafiğin ele geçirilebilmesi, okunabilmesi, hassas verilerin elde edilebilmesi gibi sonuçlara sebep olabilir. Bu kullanıma sahip mobil uygulamalar için "ATS Güvenliğinin Pasifleştirilmesi (CWE-319)" açıklığı vardır denir. ATS güvenliğinin pasifleştirilmesi sadece geliştirme ortamında önerilir, canlı (production) ortamda önerilmez.

Kurum mobil uygulamada ATS (App Transport Security) güvenliğinin pasifleştirildiği tespit edilmiştir:

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

Açıklığın Önlemi:

ATS ayarı mobil uygulama trafiğinin şifreli ve güvenli kalması için pasifleştirilmemelidir. ATS güvenliğinin pasifleşmesini düzeltmek ve tekrardan aktifleştirmek için iOS (swift veya objective-c) mobil uygulamalarda info.plist konfigürasyon dosyasında gösterilen bloğun kaldırılması yeterlidir.

info.plist:

```
...

<!-- Silinecek Kod Bloğu - Başlangıç -->

<key>NSAppTransportSecurity</key>
<dict>
  <key>NSAllowsArbitraryLoads</key>
  <true/>
</dict>

<!-- Silinecek Kod Bloğu - Son -->

...
```

Eğer http üzerinden haberleşmesi zorunlu web servisler mevcutsa tümüyle http üzerinden haberleşme ayarını açmak yerine NSAppTransportSecurity anahtarına ilgili web servis alan adını istisna olarak ekleme yolu takip edilebilir ve sadece ilgili adres (veya adresler) üzerinden http bağlantılarına izin ver, diğerlerine izin verme yapılandırması sağlanabilir. Bu yapılandırma info.plist konfigürasyon dosyasında NSAppTransportSecurity anahtarına gösterildiği gibi istisna satırları eklenerek yapılabilir:

info.plist:

```
...  
  
<key>NSAppTransportSecurity</key>  
<dict>  
  <key>NSExceptionDomains</key>  
  <dict>  
    <key>birsiteadi.com</key>  
    <dict>  
  
      <!-- TR: Subdomain'lere izin vermek için dahil et. -->  
      <!-- EN: Include to allow subdomains. -->  
      <key>NSIncludesSubdomains</key>  
      <true/>  
  
      <!-- TR: HTTP taleplere izin vermek için dahil et. -->  
      <!-- EN: Include to allow HTTP requests. -->  
      <key>NSTemporaryExceptionAllowsInsecureHTTPLoads</key>  
      <true/>  
  
      <!-- TR: Minimum TLS versiyonunu belirtmek için dahil et. -->  
      <!-- EN: Include to specify minimum TLS version. -->  
      <key>NSTemporaryExceptionMinimumTLSVersion</key>  
      <string>TLSv1.2</string>  
  
    </dict>  
  </dict>  
</dict>  
  
...
```

HTTP üzerinden erişim izni için mümkün olduğunca az istisna adres eklemelidir. Bu ayarlar neticesinde mobil uygulama trafiği güvenli hale gelecektir.

Referanslar:

1. <https://cwe.mitre.org/data/definitions/319.html>
2. <https://tr.wikipedia.org/wiki/Kanonik>
3. <https://guides.codepath.com/ios/App-Transport-Security>
4. <https://sdks.support.brightcove.com/ios/framework/working-app-transport-security-ats.html>
5. <https://stackoverflow.com/questions/30731785/how-do-i-load-an-http-url-with-app-transport-security-enabled-in-ios-9>
6. <https://medium.com/etiya/app-transport-security-ats-sorunun-%C3%A7%C3%B6z%C3%BCm%C3%BC-5778f1eb4bb>
7. <https://developers.google.com/admob/ios/app-transport-security>