

1.1.1 Kalıcı Bağlantı Dizesi (Persistent Connection String) (CWE-257)

Açıklık Önem Derecesi: Orta

Açıklığın Etkisi: Hassas Bilgilerin Ele Geçmesi

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Bir uygulamayı güvenli hale getirirken veri kaynaklarına erişimi koruma en önemli hedeflerden biridir. Bir veri kaynağına (veritabanına) bağlanmayı sağlayan bağlantı dizesi güvenli hale getirilmemişse potansiyel olarak bir açıklık sunar. Bağlantı dizelerini düz metin (plain-text) halinde saklamak veya bellekte / diskte tutmak (persist) tüm sistemi riske atabilir.

.NET ve ASP.NET uygulamalarda bağlantı dizelerinde Persist Security Info adında bir bayrak (flag) vardır. Bu bayrak true veya false değeri alır. True ya da False alması önyüzde (front-end'te) bir fark oluşturmaz, fakat arkaplanda (background'da) bir fark oluşturur. Persist Security Info=True olduğunda bağlantı dizesindeki hassas veri (örn; kullanıcı adı ve/veya parola) arka uçtaki Windows veritabanı sunucusuna gönderilir ve Windows veritabanı sunucusu gelen parolayı belleğine alır (cache'ler). Böylece sonraki gelecek bağlantılarda parolayı hatırlayabilir. Persist Security Info=False olduğunda ise bağlantı dizesindeki hassas veri (örn; kullanıcı adı ve/veya parola) arka uçtaki Windows veritabanı sunucusuna gönderilir, fakat bu sefer veriler Windows veritabanı sunucusu belleğinde tutulmaz (cache'lenmez).

Persist Security Info=True kullanımı önerilmemektedir. Çünkü True ile kullanılırsa Windows veritabanı sunucusuna sistem seviyesinde olası başarılı bir sızma girişimi gelecekte yaşandığında belleği okuyan saldırgan parolayı elde edip veritabanı uygulamasına da giriş yapabilir hale gelebilir. Yani saldırı derinliğini arttırabilir.

.NET / ASP.NET uygulamalar bağlantı dizelerinde Persist Security Info=True içerdiklerinde güvenlik açıklıklı olarak ele alınırlar. Kurum uygulamada Kalıcı Bağlantı Dizesi (CWE-257) açıklığı tespit edilmiştir:

::::BULGU::::

Açıklığın Önlemi:

Uygulamalarda bu açıklığı kapamak için şu uygulanabilir:

- Açık bir şekilde Persist Security Info bayrağına False değeri atayın ya da açıkça tanımını girmeyin ve bağlantı dizesindeki varsayılan değeri ile (yani False değeri ile) kullanımını uygulayın.
- Eğer Persist Security Info'nun True olması (örn; uygulama geliştirme fazında) gerekiyorsa gerekliliği ortadan kalktığında bu bayrağı mutlaka silin ya da False değeri atanacak şekilde ayarlamaya gidin.

ASP.NET web uygulamalarda web.config dosyalarında yer alan bağlantı dizeleri için güvensiz ve güvenli kullanımlar şu şekildedir:

Web.config - Güvensiz Yapılandırma:

```
<!-- Güvensiz Yapılandırma -->
<?xml version="1.0"?>
<configuration>
    ...
    <ConnectionStrings>
        <add name="..." connectionString="...; Persist Security Info=True; ..."
        providerName="...">
    </ConnectionStrings>
    ...
</configuration>
```

Web.config - Güvenli Yapılandırma:

```
<!-- Güvenli Yapılandırma -->
<?xml version="1.0"?>
<configuration>
    ...
    <ConnectionStrings>
        <add name="..." connectionString="...; Persist Security Info=False; ..."
        providerName="...">
    </ConnectionStrings>
    ...
</configuration>
```

.NET / ASP.NET uygulamalarda kaynak kodda yer alan bağlantı dizeleri için güvensiz ve güvenli kullanımlar ise şu şekildedir:

.NET / ASP.NET Bağlantı Dizesi - Güvensiz Hal:

```
SqlConnectionStringBuilder builder = new SqlConnectionStringBuilder();  
builder["Data Source"] = "(local)"; // Örnek veri  
builder["Persist Security Info"] = "True";  
builder["Initial Catalog"] = "XXXXXXXXX"; // Örnek veri
```

.NET / ASP.NET Bağlantı Dizesi - Güvenli Hal (1):

```
SqlConnectionStringBuilder builder = new SqlConnectionStringBuilder();  
builder["Data Source"] = "(local)"; // Örnek veri  
builder["Persist Security Info"] = "False";  
builder["Initial Catalog"] = " XXXXXXXX "; // Örnek veri
```

.NET / ASP.NET Bağlantı Dizesi - Güvenli Hal (2):

```
SqlConnectionStringBuilder builder = new SqlConnectionStringBuilder();  
builder["Data Source"] = "(local)"; // Örnek veri  
builder["Initial Catalog"] = "XXXXXXXXX"; // Örnek veri
```

Güvenli hal olarak verilen ikinci örnekte bir tanım girilmediği için varsayılan değer (yani false değer) ile bağlantı dizesi otomatik ayarlanacaktır.

Referanslar:

1. <https://cwe.mitre.org/data/definitions/257.html>
2. <https://learn.microsoft.com/en-us/dotnet/framework/data/adonet/protecting-connection-information>