1.1.1 Başlıklar Yoluyla Bilgi İfşası (Information Exposure via Headers) (CWE-200)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Bilgi İfşası

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

İsimler ve versiyon numaraları sıklıkla belirli bir teknoloji parçasının yaşam döngüsündeki belirli bir noktayı gösterir. Belirli teknolojilerin isimlerinin ve versiyon numaralarının harici kimselere ifşa edilmesi saldırganların bilinen güvenlik açıklıklar ve mevcut zararlılar (exploit'ler) kullanarak sunucuyu nasıl daha iyi hedef tahtasına koyabileceğini öğrenmesine neden olabilir, saldırganların bu belirli teknolojileri araştırabilmelerine ve arzu edilen hedefe uygun yeni exploit'ler geliştirebilmelerine neden olabilir veya saldırganların bu belirli teknolojileri belirli bir konumda not altına alma ve anında saldırmak için bu belirli teknolojilerde yeni bir güvenlik açığının duyurulmasını beklemesi ile sonuçlanabilir. Bu v.b. nedenlerle oluşan riskleri yok etmek için dahili bilgiler ve sistem bilgilerinin ifşasının azaltılması tavsiye edilmektedir.

Bir uygulama yanıt başlıklarında (response headers) sistem bilgisi ifşa edecek şekilde yapılandırma ayarına sahip olduğunda "Başlıklar Yoluyla Bilgi İfşası (CWE-200)" açıklığına sahiptir denir. Saldırganlar bu açıklık yoluyla sistem hakkında kendi açılarından değerli bilgiler elde edebilirler.

Kurum uygulamada "Başlıklar Yoluyla Bilgi İfşası (CWE-200)" açıklığı olduğu tespit edilmiştir:

:::::BULGU:::::

Açıklığın Önlemi:

Bu açıklığın kapatılabilmesi için tavsiye edilen öneriler şu şekildedir:

- Ortamların ilgili yazılım, işletim sistemi ve diğer kullanılan teknolojilerle ilgili bilgi – örn; isimlerini, versiyonlarını, ayarlarını, … - sızdırmadığından daima emin olun.

- Özellikle IIS ve .NET sunuculardaki başlıklar söz konusu olduğunda web.config dosyası elzemdir. Eğer bir web.config dosyası yoksa sırf bu amaç için oluşturulmak zorundadır.

IIS Express sunucularda server başlığı ve x-powered-by başlığı şu web.config yapılandırması ile kaldırılabilir:

```
<!-- GÜVENLİ YAPILANDIRMA -->

<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <system.webServer>
        <security>
            <requestFiltering removeServerHeader="true" />
        </security>
        <httpProtocol>
            <customHeaders>
                <remove name="X-Powered-By" />
            </customHeaders>
        </httpProtocol>
    </system.webServer>
</configuration>
```

IIS sunucularda server başlığı şu web.config yapılandırması ile kaldırılabilir.

```
<!-- GÜVENLİ YAPILANDIRMA -->

<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <system.web>
        ...
        <httpRuntime targetFramework="4.6.1" enableVersionHeader="false" />
        ...
    </system.web>
</configuration>
```

Kestrel sunucularda c# uygulamalarda server başlığı şu şekilde kaldırılabilir.

```
// Removing Server Header from Kestrel During HostBuilder Creation

public static IHostBuilder CreateHostBuilder(string[] args) =>
    Host.CreateDefaultBuilder(args)
        .ConfigureWebHostDefaults(webBuilder =>
        {
            webBuilder.UseStartup<Startup>().UseKestrel(options =>
options.AddServerHeader = false);
        });
}
```

Not:

ASP.NET uygulamaları IIS / Windows bağımlıdırlar. Kestrel sunucusu ise ASP.NET uygulamalarının Windows, Linux, MAC'de sunulabilmesini sağlayan bir platform bağımsız çözümdür.

Referanslar:

1. https://cwe.mitre.org/data/definitions/200.html
2. https://bilisim.io/2018/10/19/nedir-bu-kestrel-web-sunucusu-artisi-eksisi-ve-daha-fazlasi/
3.