1.1.1 Hassas İşlemlerin Yetersiz Log'lanması (Insufficient Logging of Sensitive Operations) (CWE-778)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Güvenlik açıklarının saptanamaması

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Uygulamalarda oturum açma, veri tabanı bağlantısı kurma veya sorgusu çalıştırma gibi hassas işlemler gerçekleştirildiğinde bu işlemler log'lanmalıdırlar. Eğer bu v.b. hassas işlemlerin her biri log ile kayıt altına alınmazlarsa adli analiz için bir iz ortada bulunmaz ve muhtemel alakalı problemlerin nedenini veya alakalı saldırıların kaynağını keşfetme işlemi daha zor veya imkansız hale gelebilir.

Bu açıklığı somutlaştırmak için bazı kod örneklerine yer verilmiştir.

C# - Güvensiz Kod Bloğu:

```
// TUR: HttpDelete Eyleminin Yetersiz Log'lanması
// ENG: Insufficient Logging of a HttpDelete action

[HttpDelete]
[Route("/movie/{id}")]
public ActionResult HandleMovies(int id)
{
    doSomething();
}
```

C# - Güvensiz Kod Bloğu 2:

```
// TUR: Veritabanı İşleminin Yetersiz Log'lanması
// ENG: Insufficient Logging of Sensitive Operation

public void DoSomethingWith1(int id)
{
    var msg = DatabaseInstance.Delete(id);
}
```

Bu iki güvensiz kod örneğinde de hassas işlemler (birincide bir nesne silme işlemi, ikincide veri tabanı klasörü silme işlemi) gerçekleştirildiklerinde ilgili işlemlerin uygulandıklarına dair log kayıtları alınmamaktadır. Bu uygulama genelinde güvenlik seviyesini düşürücü etkiye sahiptir.

C# - Güvenli Kod Bloğu:

```
// TUR: Oturum Açma İşlemi Log'lanır
// ENG: Sensitive Operation Logged

[HttpPost]
[Route("/login")]
public ActionResult handler1_v2()
{
    doThings();
    logger.Info( "Login of user occurred");
}
```

C# - Güvenli Kod Bloğu:

```
// TUR: Veri tabanı İşlemi Log'lanır
// ENG: Sensitive Operation Logged (case2)

public void DoSomethingWith2(int id)
{
    var msg = DatabaseInstance.Delete(id);
    logger.Info( "Delete of something occurred");
}
```

Bu iki güvenli kod örneğinde ise hassas işlemler (birincide oturum açma işlemi, ikincide veri tabanı klasörü silme işlemi) gerçekleştirildiklerinde ilgili işlemlerin uygulandıklarına dair log kayıtları alınmaktadır. Bu durum uygulama geneli güvenlik seviyesini arttırır. Gelecekte yaşanabilecek olumsuz siber olaylarda geliştiricilere ve sistemcilere çözüm için kolaylık sağlar.

Uygulamalarda hassas işlemler log'lanmadıklarında "Hassas İşlemlerin Yetersiz Log'lanması (CWE-778)" açıklığı vardır denir. Kurum uygulamada bu açıklık tespit edilmiştir.

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

Açıklığın Önlemi:

Önlem tavsiyeleri şu şekildedir:

- Çoklu detay seviyelerine sahip bir log mekanizması kullanılmalıdır.
- Prod ortamda uygun log'lama seviyesinin ayarlandığından emin olunmalıdır.
- Sistem yöneticilerinin saldırıları saptayabilmesi, hataları ayıklayabilmesi ve saldırı sonrası saldırının etkilerinden kurtarabilmesi için yeterli derecede veri log'lanmalıdır.

Referanslar:

1. https://cwe.mitre.org/data/definitions/778.html