1.1.1 İstisnaların Yetersiz Log'lanması (Insufficient Logging of Exceptions) (CWE-778)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Güvenlik açıklarının saptanamaması

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Uygulamalarda zaman zaman uygulamaların normal akışını bozan istisnalar (exception'lar) meydana gelebilmektedir. Güvenlik aktivitelerinden gelen istisnalar (exception'lar) meydana geldiğinde uygulama güvenliğine dönük bilgiler fırlamış olmaktadır (throw edilmiş olmaktadır). Güvenlik aktivitelerinden gelen istisnaların (exception'ların) log dosyalarında kayıt altına alınması güvenliğe dokunan olaylarının geçmişe dönük takibini sağlayacaktır, güvenlik olaylarının kaynağını ve sonuçlarını incelemede adli analiz unsuru sunacaktır ve saldırıları sınırlandırma noktasında zamanında aksiyon alınmasına yardımcı olacaktır. Eğer güvenlik aktivitelerinden gelen istisnalar log dosyalarında kayıt altına alınmazsa bu bir güvenlik açığı olarak ele alınır. Çünkü güvenliğin sağlanması noktasında bu temel unsurlardan uygulama mahrumdur. Uygulama bu önlemden mahrum kaldığında gerekli güvenlik kontrollerini ekleme aksiyonları yapılamayacağı için savunmasız kalacaktır.

Kurum uygulamasında güvenlik aktivitelerinden gelen istisnalar (exception'lar) fırladığında log kayıtlarının alınmadığı (::::::::::::veya log kayıtlarının yeterli detayda alınmadığı:::::::::::::::) tespit edilmiştir:

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

Güvenlik aktivitelerinden gelen istisnaları log'lama uygulamada güvenliği arttırıcı bir unsurdur. Eksikliği ise güvenlik seviyesini azalttığı için bir güvenlik açığı olarak ele alınır. Kurum uygulamasında güvenlik aktivitelerinden gelen istisnaların log'lanmaması uygulamayı ileride gelebilecek saldırılar neticesinde savunmasız bırakacaktır. Log'lama protokolü takip edilirse olası güvenlik aktivitelerinden gelebilecek istisnaları tetikleyen girişimler meydana geldiğinde rutin log incelemeleri sırasında güvenlik zafiyetleri tespit edilebilir ve buradan hareketle güvenlik önlemleri alınarak uygulama gelecekte gelebilecek siber saldırılara karşı korunabilir.

Açıklığın Önlemi:

Her bir fırlatılan (throw edilen) “güvenlik istisnası” (security exception) bir log alma metodu yardımıyla log'lanmalıdır. Ayrıca güvenlik istisnaları detayları asla uygulama ekranına basılmamalıdır.

Referanslar:

1. https://cwe.mitre.org/data/definitions/778.html
2. http://www.upv.es/~jgonsol/tutorial/java/exceptions/definition.html
3. https://whatis.techtarget.com/definition/exception
4. https://www.educative.io/edpresso/what-is-the-printstacktrace-method-in-java