

R – Repudiation (İnkâr Etme)

Hedef: Bir eylemi veya işlemi gerçekleştirdikten sonra, bu eylemi yaptığına dair kanıtları yok ederek sorumluluğu inkâr etmek.

1. Saldırı Ağacı – Transaction Log Silme

Hedef: Kritik Bir Değişikliğin Sorumluluğunu İnkâr Etmek

Adım 1: CSMS Sunucusuna Yetkili Erişim Sağlamak

Alt Adım 1a: Çalınan bir admin parolası ile CSMS'e bağlanmak.

Alt Adım 1b: Başka bir zafiyet (örn. RCE) ile sunucuda root yetkisi elde etmek.

Adım 2: Kötü Amaçlı Eylemi Gerçekleştirmek

Alt Adım 2a: Ağdaki tüm istasyonlara "kapatma" (ChangeAvailability: Unavailable) komutu göndermek.

Adım 3: Denetim (Audit) Kayıtlarına Erişmek

Alt Adım 3a: Sunucudaki /var/log/csms_audit.log dosyasına veya audit_logs veritabanı tablosuna erişmek.

Adım 4: Kanıtları Yok Etmek

Alt Adım 4a: Kendi IP adresi ve kullanıcı adıyla ilişkili tüm log satırlarını silmek veya değiştirmek.

Sonuç: Olay incelendiğinde, "tüm istasyonları kimin kapattığına" dair bir kanıt bulunamaz.

2. Sömürü Senaryoları

Transaction Log Silme: (Yukarıdaki ağaçta açıklandı).

Non-Repudiation (İnkâr Edilemezlik) Zayıflığı: Bir kullanıcı, mobil uygulama üzerinden şarjı başlatır. Ancak işlem kaydı (örn. StartTransaction) CSMS'e ulaşmaz veya veritabanına yazılırken bir hata oluşur. Kullanıcı şarj alır. Ay sonunda fatura gelince "Ben bu şarjı yapmadım" der ve CSMS'in elinde bunu kanıtlayacak imzalı bir dijital kayıt bulunmaz.

3. Azaltma Stratejileri (Mitigation)

Harici ve Değişmez (Immutable) Loglama: Tüm kritik işlem ve denetim loglarının, CSMS sunucusundan ayrı, WORM (Write-Once, Read-Many) özelliğine sahip veya silme yetkisi kısıtlanmış merkezi bir SIEM (Security Information and Event Management) sistemine gerçek zamanlı olarak gönderilmesi.

Kriptografik Kayıt (Non-repudiation): Kritik işlemlerin (özellikle ISO 15118 ile yapılan ödeme ve şarj sözleşmelerinin) araç ve istasyon tarafından dijital olarak imzalanması.

Ayrıcalıkların Ayrılığı (SoD): Normal bir adminin logları sadece "okuyabilmesi", ancak "silememesi" veya "değiştirememesi". Log yönetimi yetkisinin sadece ayrı bir "Audit" (Denetçi) rolüne verilmesi.

4. Tespit Mekanizmaları (Detection)

Log Akış İzleme: SIEM sisteminin, bir CSMS sunucusundan 5 dakikadan uzun süredir log gelmemesi durumunda (log servisinin durdurulmuş veya sunucunun kapanmış olabileceğine işaret eder) alarm üretmesi.

Dosya Bütünlük İzleme (FIM): Sunucu üzerinde çalışan bir FIM aracının, /var/log dizinindeki dosyalarda herhangi bir "silme" veya "değiştirme" (modification) tespiti anında alarm üretmesi.

R - Repudiation DREAD Değerlendirmesi

(CSMS'i ele geçiren bir adminin/saldırganın, yaptığı kötücül eylemlerin (örn. tüm istasyonları kapatma) izlerini silmesi.

D - Damage Potential (Zarar Potansiyeli): 6

Gerekçe: Doğrudan bir zarara yol açmaz, ancak başka bir saldırının (örn. bir adminin tüm istasyonları kapatması) *kanıtını* yok eder. Adli bilişim (forensics) sürecini imkansız hale getirir, sorumluların bulunmasını engeller.

R - Reproducibility (Tekrarlanabilirlik): 8

Gerekçe: Saldırgan sunucuda root veya veritabanında admin yetkisine sahipse, logları silmesi %100 tekrarlanabilir bir işlemdir (eğer WORM loglama yoksa).

E - Exploitability (İstismar Edilebilirlik): 7

Gerekçe: Öncülü zordur (sunucuda root yetkisi almak). Ancak bu yetki alındıktan

sonra logları silmek (rm /var/log/audit.log) çok kolaydır.

A - Affected Users (Etkilenen Kullanıcılar): 1

Gerekçe: Doğrudan sadece operatör (şirket) etkilenir, çünkü bir olayı araştıramaz hale gelirler.

D - Discoverability (Keşfedilebilirlik): 2

Gerekçe: Logların silinebilir olması bir "zafiyet" değildir, sistemin bir özelliğidir (eğer WORM/immutable loglama yoksa). Zafiyet, loglara erişimi sağlayan (örn. RCE) asıl zafiyettir.

Risk Skoru: 24/50 (Orta Risk)

Sacide Aışenur Direk