Vulnerability Assessment Report Template

**Ime i prezime: Milica Đumić  
Tim:7  
Datum: 27.10.2024.  
Scan Tool:** Nessus (10.8.3)  
**Test okruženje:** Metasploitable3

### **1. Enumeracija CVE-a**

* **CVE ID: 2016-9794**
* **Opis:**Podsistem u jezgru Linux-a, pre 4.7, sadrži race condition koja dozvoljava korisnicima da izvedu denial of service (pad sistema) ili nespecificirani uticaj korišćenjem određenih komandi. Ovo je otkriveno u podsistemu Advanced Linux Sound Architecture (ALSA).

### **2. CVSS skor**

* **CVSS skor (numerička vrednost): 7.8**
* **Vektor: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H**

CVSS:3.1 = Ocena se dobija korišćenjem CVSS 3.1

AV = Attack Vector: Local (Eksploatacija se može dogoditi lokalno, npr. čitanje/pisanje u lokalnom fajl sistemu)

AC = Attack Complexity: Low (Ovaj napad ne zahteva mnogo tehničkog znanja, lako ga je izvesti)

PR = Privileges Required: Low (Napadaču su potrebne privilegije i napada neosetljive resurse)

UI = User Interaction: None (Za korišćenje ranjivog sistema nije potreban niko drugi sem napadača)

S = Scope: Unchanged (Opseg ranjivosti nije promenjen)

C = Confidentiality Impact: High (Napadač dobija informacije koje bi trebale biti zaštićene, narušava se poverljivost)

I = Integrity Impact: High (Napadač može da menja podatke i fajlove, narušen integritet)

A = Availability Impact: High (Napadač može da ograniči legitimni pristup sistemu, narušena dostupnost)

* **Opravdanje:**Posledice ovog napada su izmena i pristup zaštićenim fajlovima, potencijalno pad kompletnog sistema. Kompelksnost napada je mala, a pomenute posledice mogu biti katastrofalne po sistem tako da je to doprinelo veličini ocene za ovaj napad. CIA trijada (poverljivost, integritet i doslednost) su osobine koje su narušene na visokom nivou, a veoma su bitne za konzistentan i bezbedan rad sistema i one takođe učestvuju u formiranju velike ocene ovog napada.

### **3. Dostupnost eksploita**

* **Postoji javno dostupan eksploit (Da/Ne):**Ne postoji.
* **Opis eksploita:**
* **Kod eksploita (ukoliko postoji):**

### **4. Analiza uzroka (root cause)**

* **Uvođenje Greške (Commit/Verzija):**

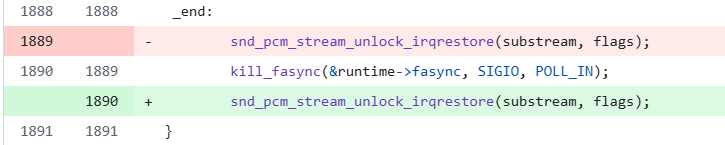
Boazen Ding je otkrio ovu ranjivost. Commit je objavljen 14.04.2016. godine i odnosi se na sve verzije jezgra Linux-a pre 4.7.

U funkciji snd\_pcm\_period\_elapsed() se poziva funkcija kill\_fasync(), ali van zaključavanja toka podataka. Na ovom mestu je moguće da se dogodi trka do podataka (race condition).

* **Primer Koda (ako je primenljivo):**

### **5. Preporuke za mitigaciju**

* **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
* **Mitigation Strategy:**Pomeranje poziva funkcije kill\_fasync() nakon zaključavanja toka će na jednostavan način rešiti ovaj problem. Interfejs fasync se retko koristi, tako da ovo ne bi trebalo da ima veliki uticaj na performanse, ali bi trebalo da pokrije veliki broj slučajeva. U idealnom slučaju bi trebalo da se implementira mehanizam sinhronizacije za ispravan rad toka.



* **Alternativni fix (ukoliko ne postoji vendorski):**