Vulnerability Assessment Report

**Ime i prezime: Ratko Šebez  
Tim: 1  
Datum: 29.10.2024.  
Scan Tool:** Nessus (10.8)  
**Test okruženje:** Metasploitable3

**1. Enumeracija CVE-a**

* **CVE ID: CVE-2014-3634**
* **Opis:**  
  Ova ranjivost odnosi se na napredni logging sistem rsyslog. On se koristi da prikupi, filtrira, formatira i čuva log poruke iz raznih aplikacija i servisa. Proširuje mogućnosti sistema syslog.  
  Ranjive su verzije pre 7.6.6. Najčešći napad je denial of service, ali moguće je izvesti i neke druge tipove napada.

**2. CVSS skor**

* **CVSS skor (7.5):**
* **Vektor:** AV:N/AC:L/Au:N/C:P/I:P/A:P  
  AV (attack vector): Network - eksploatacija se može dogoditi preko mreže kao što je internet  
  AC (attack complexity): Low - napad je lako izvesti i ne zahteva mnogo tehničkog znanja  
  AU (authentication): None - napadač ne mora da se autentifikuje da bi izveo napad  
  C (confidentiality): Partial - delimično je narušena poverljivost  
  I (integrity): Partial - delimično je narušen integritet  
  A (availability): Partial - delimično je narušena dostupnost
* **Opravdanje:**  
  Ova ranjivost ima visok CVSS skor zbog više faktora. Napadač ne mora imati mnogo tehničkog znanja da bi izveo napad. Takođe, napad je moguće izvesti preko mreže i nije potrebna autentifikacija. Ovo znači da je broj potencijalnih napadača velik i da je relativno lako izvesti ga.  
  Visok CVSS skor dolazi i iz faktora da se ovim napadom delimično može narušiti svaka stavka iz CIA trijade.

**3. Dostupnost eksploita**

* **Postoji javno dostupan eksploit (Da/Ne): Da**
* **Opis eksploita:**  
  Ranjivost se aktivira tako što se pošalje log poruka sa nevalidnom PRI vrednosti. Potrebno je da je PRI veći od 191.  
  Posledica uspešnog napada je najčešće denial of service.

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

* **Uvođenje Greške (Commit/Verzija):**  
  U sistemskom heder fajlu postoji definicija koja postavlja maksimalni broj "facility" vrednosti na 24. LOG\_FACMASK dozvoljava vrednosti do 1016.   
  Kada Rsyslog obradi log poruku sa PRI vrednošću iznad dozvoljenih 191, dolazi do prekoračenja granica niza (array overflow), jer sistem pokušava da pristupi elementima niza koji ne postoje. To izaziva greške i može dovesti do prekida rada usluge (denial of service).
* **Primer Koda (ako je primenljivo):**

<https://www.rsyslog.com/remote-syslog-pri-vulnerability/>  
#define LOG\_NFACILITIES 24 /\* current number of facilities \*/

#define LOG\_FACMASK 0x03f8 /\* mask to extract facility part \*/

/\* facility of pri \*/

#define LOG\_FAC(p) (((p) & LOG\_FACMASK) >> 3)

**5. Preporuke za mitigaciju**

* **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
* **Mitigation Strategy:**  
  Strategija za rešavanje ranjivosti jeste unapređenje verzije rsyslog sistema. Ranjivost je otklonjena u verziji 7.6.6. Ažuriranje se može izvesti komandom "sudo apt install rsyslog".  
  Ukoliko je iz nekog razloga nemoguće ažurirati verziju sistema, napad se može sprečiti limitiranjem pristupa postavkom firewall-a.

**1. Enumeracija CVE-a**

* **CVE ID: CVE-2018-18751**
* **Opis:**  
  Ova ranjivost odnosi se na napredni GNU gettext. To je skup alata i biblioteka namenjenih za internacionalizaciju i lokalizaciju softverskih aplikacija. Glavna svrha gettext-a je da omogući programerima da upravljaju prevodima tekstualnih poruka u softveru, kao što su greške, poruke u korisničkim interfejsima i uputstva.  
  Ranjivost je otkrivena u GNU gettext 0.19.8 verziji. Ranjivost može prouzrokovati denial of service zbog double free greške u funkciji default\_add\_message u fajlu read-catalog.c.

**2. CVSS skor**

* **CVSS skor (9.8):**
* **Vektor:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H  
  AV (attack vector): Network - eksploatacija se može dogoditi preko mreže kao što je internet  
  AC (attack complexity): Low - napad je lako izvesti i ne zahteva mnogo tehničkog znanja  
  PR (priviliges required): None - napadač ne mora da se autentifikuje da bi izveo napad  
  UI (user interaction): None - napad ne zahteva interakciju drugog korisnika  
  S (scope): Unchanged - ranjivost samo narušava rad gettext-a, ne i nekih drugih sistema  
  C (confidentiality): High - visoko narušena poverljivost  
  I (integrity): High - visoko narušen integritet  
  A (availability): High - visoko narušena dostupnost
* **Opravdanje:**  
  Ova ranjivost ima visok CVSS skor zbog više faktora. Napadač ne mora imati mnogo tehničkog znanja da bi izveo napad. Takođe, napad je moguće izvesti preko mreže i nije potrebna autentifikacija. Ovo znači da je broj potencijalnih napadača velik i da je relativno lako izvesti ga. Napad ne zahteva interakciju sa drugim korisnikom.  
  Visok CVSS skor dolazi i iz faktora da se ovim napadom može narušiti svaka stavka iz CIA trijade.

**3. Dostupnost eksploita**

* **Postoji javno dostupan eksploit (Da/Ne): Ne**

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

* **Uvođenje Greške (Commit/Verzija):**  
  Ranjivost je otkrivena u GNU gettext 0.19.8 verziji. Ranjivost može prouzrokovati denial of service zbog double free greške u funkciji default\_add\_message u fajlu read-catalog.c.

**5. Preporuke za mitigaciju**

* **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
* **Mitigation Strategy:**  
  Preporučeno je da se ažurira ceo sistem, a ne samo biblioteka gettext. U slučaju Ubuntu operativnog sistema potrebno ga je ažurirati na verziju 12.04 ili više. Uneti komandu "sudo apt-get update".  
  Ranjivost se može otkloniti i ažuriranjem same biblioteke na verziju 0.20.2 ili višu komandom "sudo apt install rsyslog".

**1. Enumeracija CVE-a**

* **CVE ID: CVE-2014-8769**
* **Opis:**  
  Ova ranjivost odnosi se na alat za analizu paketa tcpdump. On se koristi za prikupljanje i analizu mrežnog saobraćaja na računarskoj mreži. Omogućava korisnicima da presreću i beleže saobraćaj koji prolazi kroz mrežni interfejs.  
  Ranjivost postoji u verzijama između 3.8 i 4.6.2. Udaljeni napadač može da dobije pristup poverljivim informacijama iz memorije ili da izazove denial of service napad.

**2. CVSS skor**

* **CVSS skor (6.4):**
* **Vektor:** AV:N/AC:L/Au:N/C:P/I:N/A:P  
  AV (attack vector): Network - eksploatacija se može dogoditi preko mreže kao što je internet  
  AC (attack complexity): Low - napad je lako izvesti i ne zahteva mnogo tehničkog znanja  
  AU (authentication): None - napadač ne mora da se autentifikuje da bi izveo napad  
  C (confidentiality): Partial - delimično je narušena poverljivost  
  I (integrity): None - delimično je narušen integritet  
  A (availability): Partial - delimično je narušena dostupnost
* **Opravdanje:**  
  Ova ranjivost ima srednji CVSS skor zbog više faktora. Napadač ne mora imati mnogo tehničkog znanja da bi izveo napad. Takođe, napad je moguće izvesti preko mreže i nije potrebna autentifikacija. Ovo znači da je broj potencijalnih napadača velik i da je relativno lako izvesti ga.  
  Ovim napadom može parcijalno narušiti poverljivost i dostupnost.

**3. Dostupnost eksploita**

* **Postoji javno dostupan eksploit (Da/Ne): Ne**

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

* **Uvođenje Greške (Commit/Verzija):**  
  Ranjivost je otkrivena u tcpdump verzijama između 3.8 i 4.6.2. Udaljenim napadačima je omogućeno da dobiju osetljive informacije iz memorije ili izazovu denial of service putem "crafted Ad hoc On-Demand Distance Vector (AODV)" paketom koji izaziva pristup memoriji van dozvoljenih granica.

**5. Preporuke za mitigaciju**

* **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
* **Mitigation Strategy:**  
  Ranjivost se može otkloniti i ažuriranjem tcpdump paketa na verziju 4.6.3 ili višu komandom "sudo apt install tcpdump".