Vulnerability Assessment Report Template

Ime i prezime: Katarina Vučić R228/2024
Tim: 3
Datum: 26.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

Sve korake ispod treba ponoviti za svaku ranjivost

---

1. Enumeracija CVE-a

- **CVE ID: 51192**

- **Opis:**
  Ukratko upišite ranjivost i način na koji ona pogađa servis. Dajte detaljne informacije o servisu (npr., ime servisa, port, protokol…).

  Naziv ranjivosti: SSL sertifikatu se ne može vjerovati

  Nessus alat navodi da se ova ranjivost može desiti na 3 različita načina, gdje se lanac povjerenja može razbiti:

  1. Vrh sertifikatskog lanca (ili stabla) nije potomak poznatog javnog CA (certificate authority). Može se desiti ako korijen stabla sertifikata nije poznat ili ako je to self-signed sertifikat (sertifikat koji sam sebe potpisuje). Takođe, može se desiti i ako posrednički (intermediate) sertifikat nedostaje, koji bi povezao vrh sertifikatskog lanca sa CA.
  2. U lancu/stablu sertifikata postoji sertifikat koji nije validan.
  3. U lancu/stablu sertifikata se nalazi potpis koji se ne poklapa sa informacijama datog sertifikata ili jednostavno nije mogao biti verifikovan. Ovo se može riješti tako što će izdavalac (issuer) ponovo potpisati sertifikat. Potpisi koji ne mogu biti verifikovani su rezultat toga što izdavalac sertifikata koristi algoritam za potpisivanje koje Nessus ili ne podržava ili ne prepoznaje.

  Ako je remote host javan u toku produkcije, svaki prekid lanca sertifikata čini teže korisnicima da verifikuju autentičnost i identitet veb servera. Ovo bi moglo da olakša realizaciju man-in-the-middle napada.

Port: 631 /tcp / www

Servis: IPP (Internet Printing Protocol)

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 6.5 (medium)
- **Vektor:**
  Opišite vektor string (npr. `AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`) opišite svaku pojedinačnu komponentu.
  Vektor: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
  AV – Attack Vector. Opisuje kako ranjivost može biti eksploatisana. Vrijednost – N (Network). Napadač može da eksploatiše ranjivost i kada je udaljen, putem interneta. Ovaj tip ranjivosti je generalno rizičniji.
  AC – Attack Complexity (kompleksnost napada). Opisuje koliko je kompleksno da se ranjivost eksploatiše. Vrijednost: L (low). Označava da je ranjivost lako eksploatisati. Predstavlja visok rizik.
  PR – Privileges Required (zahtjevane privilegije). Opisuje da li napadač treba određene privilegije da bi eksploatisao ranjivost. Vrijednost: N (None). Označava da nisu potrebne nikakve privilegije. Takođe, povećava rizik za napade.
  UI – User Interaction (interakcija korisnika). Govori da li je napadaču potrebna pomoć od strane korisnika da bi se ranjivost eksploatisala. Vrijednost: N (None). Nije potrebna pomoć korisnika. Povećava rizik.
  S – Scope. Definiše scope uspješnog napada (da li će djelovati samo na ranjivu komponentu ili ima uticaja i na ostale komponente). Vrijednost: U (unchanged). Znači da utiče samo na ranjivu komponentu. Ovo ograničava pogođenu površinu, na taj način je manji uticaj na cijeloukupan sistem.
  C – Confidentialty (povjerljivost). Definiše uticaj na povjerljivost podataka. Vrijednost: L (low). Povjerljivost može biti kompormitovana, izloženost je ograničena i samo neki podaci su pod rizikom. Niska izloženost povjerljivosti daje manji rizik za izlaganje povjerljivih podataka.
  I – Integrity (integritet). Definiše uticaj na integritet podataka (da li podaci mogu biti izmijenjeni). Vrijednost: L (low). Integritet podataka može biti kompromitovan, ali sa manjim posljedicama po sistem i organizaciju (uključujući i korisnike sistema).
  A – availability (dostupnost). Definiše da li ranjivost može uticati na dostupnost servisa. Vrijednost: N (None). Ranjivost ne predstavlja opasnost po dostupnost servisa.
- **Opravdanje:**
  Zašto ova ranljivost ima dodeljen ovaj CVSS skor? Diskutujte o faktorima kao što su eksploatabilnost, impact i obim ranljivosti.

  U nastavku teksta će biti objašnjeno zašto je 6.5 skor dodijeljen ovoj ranjivosti.

Ova ranjivost može biti lako eksploatisana (može biti eksploatisana putem interneta), sa vrlom malom kompleksnošću, bez potrebe za posebnim privilegijama ili interakcijom korisnika. Međutim, uticaj je ograničen samo na ranjivu komponentu, narušavanje povjerljivosti, integriteta podataka i dostupnosti servisa je malo. Ovaj rezultat održava balans između veoma lake ekspolatacije ranjivosti i relativno umjerenog uticaja na bezbjednost sistema.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Izvršite pretragu (npr. Exploit-DB, GitHub, blog postovi) za javno dostupan eksploit koji je vezan za ovaj CVE.

  Ne postoji eksploit koji je direktno vezan za Nessus Plugin ID 51192, ali postoje razni eksploiti vezani za SSL/TLS ranjivosti ili nepravilno rukovođenje sertifikatima.
- **Opis eksploita:**
  Ako postoji eksploit, navedite detalje o tome kako funkcioniše, šta cilja, i koje su potencijalne posledice uspešnog napada.
  Man-in-the-Middle – napadač prekida komunikaciju. Napadač može da podmetne zamku pomoću koje će moći uspješno da prekine komunikaciju (može npr. da podmetne svoj tajni ključ ili da napravi lažnu WI-FI adresu ,,Evil Twin"). Ovo mu pruža mogućnost neautorizovanog pristupa i izmjene podataka, kao i prosljeđivanja lažnog response-a (odgovora).
  Javno dostupni alati – postoje razni javno dostupni alati za eksploataciju problema sa validacijom sertifikata u TLS/SSL konfiguraciji.

- **Kod eksploita (ukoliko postoji):**
  Objasnite srž eksploita, dajte screenshot koda (samo glavni dio)

  Isječci koda alata SSLStrip (https://github.com/moxie0/sslstrip/) koji izvršava Man-in-the-Middle napad:

  Slika 1 prikazuje kod gdje se HTTPS komunikacija mijenja za HTTP komunikaciju.

```
def replaceSecureLinks(self, data):
    iterator = re.finditer(ServerConnection.urlExpression, data)

    for match in iterator:
        url = match.group()

        logging.debug("Found secure reference: " + url)

        url = url.replace('https://', 'http://', 1)
        url = url.replace('&amp;', '&')
        self.urlMonitor.addSecureLink(self.client.getClientIP(), url)

    data = re.sub(ServerConnection.urlExplicitPort, r'http://\1/', data)
    return re.sub(ServerConnection.urlType, 'http://', data)
```

Slika 1 Zamjena HTTPS za HTTP

Slika 2 prikazuje eksploataciju potencijalno povjerljivih podataka sa servera.

```
def handleResponse(self, data):
    if (self.isCompressed):
        logging.debug("Decompressing content...")
        data = gzip.GzipFile('', 'rb', 9, StringIO.StringIO(data)).read()

    logging.log(self.getLogLevel(), "Read from server:\n" + data)

    data = self.replaceSecureLinks(data)

    if (self.contentLength != None):
        self.client.setHeader('Content-Length', len(data))

    self.client.write(data)
    self.shutdown()
```

Slika 2 Eksploatacija podataka

4. Analiza uzroka (root cause)

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

  Istražite kako je ranljivost uvedena. Identifikujte verziju, tačan commit, ili biblioteku koja je izazvala ranljivost (npr. "Uvedeno u verziji X zbog neadekvatne validacije u biblioteci Y").

  Istorijat:

  Verzija plugin-a: 1.19

  Datum objavljivanja: 15.12.2010.

  Datum posljednje izmjene: 27.4.2020.

  Kako ranjivost nastaje je objašnjeno u sekciji 1.

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

  Pružite primer koda koji je glavni krivac, ako je dostupan.

  Nije primjenljivo.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):**

  Konkretno za Metasploitable3 ne postoji patch ili vendor fix za gorenavedeni problem. Problem bi bio riješen postavljanjem validnog sertifikata.
- **Mitigation Strategy:**
  Kako se konkretno apply-uje gore navedeni fix/patch, preporuka alata koji to može odraditi automatski…

  - Kupovinom validnog sertifikata (od poznatog CA)
  - Osiguravanjem validnost lanca/stabla sertifikata.

  Takođe, postoje alati koji provjeru validnosti sertifikata rade za nas. Primjer takvog softvera je Let’s Encrypt. On osigurava da su seritifkati uvijek up-to-date.

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

  Opis kako bi se ovo moglo rešiti dobudživanjem trenutne verzije

Ažuriranjem SSL/TLS konfiguracije servera da koristi validne sertifikate, osiguravanjem da su svi dijelovi lanca sertifikata pravilno postavljeni i povjerljivi od strane klijenata.