Vulnerability Assessment Report Template

Ime i prezime: Luka Milanko
Tim: 9
Datum: 28. 10. 2024.
Scan Tool: Nessus 10.8.3
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** 2017-12615
- **Opis:** Ova ranjivost je specifična za Apache Tomcat 7 server. Ona omogućava daljinsko postavljanje datoteka i njihovo izvršavanje korišćenjem PUT metode unutar HTTP zahteva kojim se mogu slati JSP fajlovi i zatim izvršavati komande na daljinu. Ovaj server obično prima zahteve na standardnom 8080 portu.

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 8.1
- **Vektor:**
  CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  Attack Vector: Network – moguće je izvesti napad preko internet mreže
  Attack Complexity: High – potrebno je široko predznanje za realizaciju napada
  Privileges Required: None – nikakve specifične privilegije ili nalog nisu neophodni User Interaction: None – nikakva akcija korisnika nije neophodna
  Scope: Unchanged – opseg ranjivosti nije promenjen, utiče samo na ciljani sistem
  Confidentality: High – napadač može lako da pristupa poverljivim podacima
  Integrity: High – napadač može lako da menja fajlove ili podatke
  Availability: High – ova ranjivost prouzrokuje veliko ometanje rada sistema pa čak i prekid

- **Opravdanje:**
  Zbog toga što ova ranjivost ima ocene visokog rizika za poverljivost, integritet i dostupnost to znači da se podaci mogu vrlo lako menjati i eksploatisati, a da se sam sistem može u velikoj meri usporiti pa čak i prekinuti njegov rad. Za pristup sistemu i izvršavanje napada možemo koristiti internet mrežu, tj. ne moramo biti fizički povezani, što olakšava eksploatisanje. Ovaj CVSS skor takođe opravdava i to što ne moramo imati

nikakve privilegije niti nalog kao ni korisničku interakciju; napad se može izvršiti i bez korisnikovog znanja. Jedina stavka koja ide u prilog smanjenju ovog skora je to što nam za izvršavanje ovakvog napada treba visoko predznanje jer je napad kompleksan, ali kada jednom napadač uspe da uđe u sistem može da nanaese veliku štetu.

---

3. Dostupnost eksploita

● **Postoji javno dostupan eksploit (Da/Ne):** Da ●
Opis eksploita:
Ovaj eksploit omogućava slanje određenog JSP fajla pomoću PUT metode u HTTP zahtevu koji sadrži kod koji kada se izvršava na serveru može da lista sadržaje direktorijuma, menja sadržaje fajlova itd. Sam Apache Tomcat 7 server sadrži mehanizam koji sprečava primanje JSP fajlova ali se on vrlo lako zaobilazi dodavanjem '/' na putanju nakon .jsp fajla.

Kod eksploita (ukoliko postoji):
Primer zahteva koji postavlja maliciozni fajl na server:

```
PUT /myfile.jsp/ HTTP/1.1
Host: 127.0.0.1:8080
Connection: close
Content-Length: 85

<% out.write("<html><body><h3>[+] JSP upload successfully.</h3></body></html>"); %>
```

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):** Ova ranjivost se javlja u verzijama od 7.0.0 do 7.0.79. Uzrok ove ranjivosti je omogućivanje postavljanja taga <readonly> na false u konfiguraciji servleta.

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

```
<servlet>
    <servlet-name>default</servlet-name>
    <servlet-class>org.apache.catalina.servlets.DefaultServlet</servlet-class>
    <init-param>
        <param-name>debug</param-name>
        <param-value>0</param-value>
    </init-param>
    <init-param>
        <param-name>listings</param-name>
        <param-value>false</param-value>
    </init-param>
    <init-param>
        <param-name>readonly</param-name>
        <param-value>false</param-value>
    </init-param>
    <load-on-startup>1</load-on-startup>
</servlet>
```

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da
- **Mitigation Strategy:**
  Unapređivanje Apache Tomcat servera na verziju 7.0.81 ili više gde je onemogućeno ovakvo konfigurisanje servleta. Ažuriranje je najlakše obaviti tako što se obrišu stari fajlovi i preuzmu novi sa zvaničnog Apache Tomcat sajta putem linka https://tomcat.apache.org/upgrading.html

---

1. Enumeracija CVE-a

- **CVE ID:** 2012-1675
- **Opis:** Ova ranjivost je vezana za Oracle TNS Listener koji omogućava komunikaciju između klijenta i baze. Javlja se u verzijama Oracle baze podataka 11g: 11.1.0.7, 11.2.0.2, 11.2.0.3, i 10g: 10.2.0.3, 10.2.0.4, 10.2.0.5. zbog greške u implementaciji TNS Listenera što omogućava da napadač presretne komunikaciju i preusmeri je na svoju mašinu, a zatim i da je prati i šalje zahteve ka bazi. Ovaj server prima zahteve na portu 1521.

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 7.5
- **Vektor:** CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P
  Attack Vector: Network – moguće je izvesti napad preko internet mreže
  Attack Complexity: Low – napad nije težak za izvođenje
  Authentication: None – nije nam neophodan nikakav vid autentifikacije
  Confidentality: Partial – napadač može da pristupa poverljivim podacima ali ne svim
  Integrity: Partial – napadač može da menja fajlove ili podatke delimično
  Availability: Partial – ova ranjivost prouzrokuje ometanje rada sistema ali ne do tačke prekida

- **Opravdanje:**
  Za ovako visok skor je najzaslužniji vrlo jednostavan upad u komunikaciju između klijenta i servera. Napad sam po sebi nije kompleksan, moguć je pristup i sa mreže, nije nam potrebna nikakva autentifikacija. Međutim, količina štete koju napadač može da prouzrokuje je parcijalna, što donekle smanjuje ovaj skor.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):** Da
  - **Opis eksploita:**

Pošto je TNS Listener obično konfigurisan na standardnom portu 1521 napadač može lako presresti saobraćaj. Prvo šalje specijalno oblikovan zahtev koji se ponaša kao legitiman klijent. Na taj način napadač dodaje svoju sesiju u TNS-ov registar sesija. TNS Listener će sledeći put odgovore slati prvo ka napadačevom serveru i tako mu omogućiti da presreće komunikaciju ili čak i da menja instrukcije.

  - **Kod eksploita (ukoliko postoji):** Ne postoji

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):** Ova greška seže do prvih verzija Oracleovih baza podataka, tačnije do Oracle 8i.
- **Primer Koda (ako je primenljivo):**

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da
- **Mitigation Strategy:**
  Ova ranjivost je zakrpljena još 2012. godine i već kod verzije Oracle Database 11g R2 i naviše se ova ranjivost ne javlja. Unapređivanje se vrši prvo replikacijom baze a zatim i korišćenjem Oracle Database Upgrade Assistant koji će obaviti većinu poslova, uključujući migraciju podataka, ažuriranje parametara i podešavanja za novu verziju.

1. Enumeracija CVE-a

- **CVE ID:** 2017-12615
- **Opis:** Ova ranjivost je vezana za *Sambu,* softver koji služi za deljenje fajlova i štampača između različitih operativnih sistema. Ona koristi NTLMSSP protokol za razmenu poverljivih podataka. Međutim, u verzijama 3.2.0 do 4.4.0 je otkriveno da postoji bezbedonosni propust u vidu nedostatka enkripcije ili sigurnosnih tokena, što otvara prostor za man-in-the-middle napad. Samba radi na portu 445.

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 5.9
- **Vektor:**
  CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
  Attack Vector: Network – moguće je izvesti napad preko internet mreže
  Attack Complexity: High – potrebno je šire predznanje za izvođenje napada
  Privileges Required: None – nikakve specifične privilegije ili nalog nisu neophodni
  User Interaction: None – nikakva akcija korisnika nije neophodna
  Scope: Unchanged – opseg ranjivosti nije promenjen, utiče samo na ciljani sistem
  Confidentality: None – napad ne može da utiče na poverljive podatke
  Integrity: High – napadač može da menja fajlove ili podatke u velikoj meri
  Availability: None – ova ranjivost ne prouzrokuje ometanje rada sistema

- **Opravdanje:**
  Ovaj napad spada u srednje rizične zato što napadač ima ograničen uticaj na podatke (može samo da ih menja), a ne trebaju mu nikakve privilegije. S druge strane, napad nije toliko jednostavan pa to dodatno smanjuje ocenu.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):** Ne
  - **Opis eksploita:**
    Zbog bezbedonosnog propusta u načinu na koji Samba autentifikuje korisnike, gde nedostaje enkripcija pri slanju zahteva za autentifikaciju, napadač može da izvrši man-in-the-middle napad i presreće saobraćaj. Kada napadač presretne ove zahteve, može da analizira saobraćaj u pokušaju da otkrije korisničke kredencijale.
  - **Kod eksploita (ukoliko postoji):** Ne postoji

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):** Ova greška se javlja kod verzija *Sambe* od 3.2.0 do 4.4.0
- **Primer Koda (ako je primenljivo):**

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da
- **Mitigation Strategy:**
  Od verzije 4.4.14 pa na dalje ova ranjivost je zakrpljena. Unapređivanje Sambe na verziju otpornu na ovu ranjivost se vrši preuzimanjem ove verzije sa zvaničnog sajta https://www.samba.org/