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:** CVE-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:HAttack 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):**

****

### **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