Vulnerability Assessment Report Template

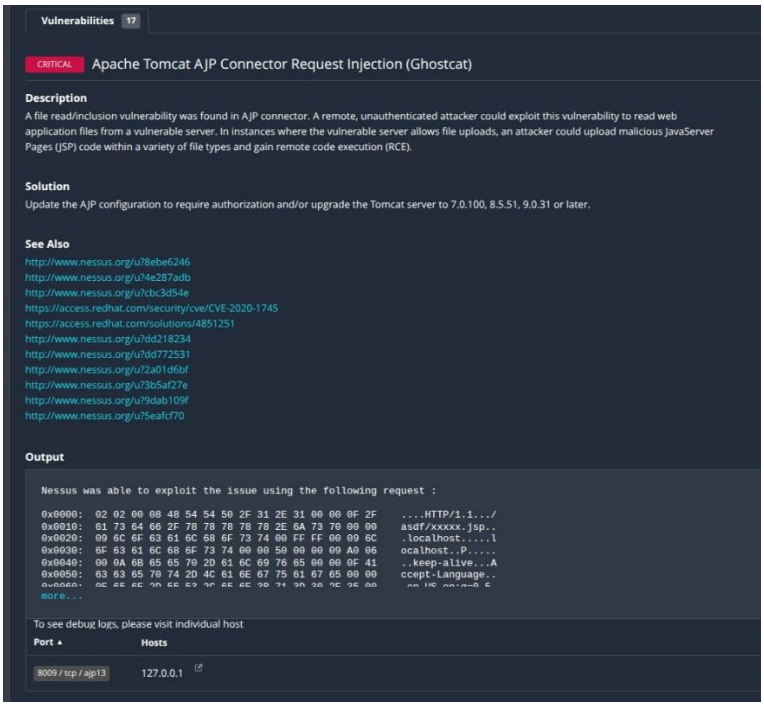
Ime i prezime: Dušica Trbović
Tim: ?
Datum: 21.12.2025.
Scan Tool: Nessus (10.11.1 (#21) LINUX)
Test okruženje: Metasploitable

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2020-1938 (Ghostcat)
  (u Nessusu se pojavljuje zajedno sa CVE-2020-1938, a u nekim referencama i CVE-2020-1745 – ali primarni i najpoznatiji je CVE-2020-1938)

- **Opis:**
  Ranjivost CVE-2020-1938, poznata pod nazivom Ghostcat, pogađa Apache Tomcat AJP (Apache JServ Protocol) konektor. Problem nastaje kada je AJP servis izložen bez adekvatne autentifikacije, što omogućava udaljenom, neautentifikovanom napadaču da čita proizvoljne fajlove sa servera. U određenim konfiguracijama, posebno kada su omogućeni upload mehanizmi ili dinamičko izvršavanje JSP fajlova, ova ranjivost može dovesti i do udaljenog izvršavanja koda (RCE). U testiranom sistemu, Nessus je detektovao da je ranjivi AJP servis aktivan na portu 8009/tcp, što omogućava eksploataciju ranjivosti sa udaljene lokacije.



- Detalji o servisu:
    - Servis: Apache Tomcat AJP Connector
    - Protokol: AJP (Apache JServ Protocol)
    - Port: 8009/tcp
    - Tip ranjivosti: File Disclosure / Remote Code Execution
    - Pristup: Remote, bez autentifikacije

  Ranjivost predstavlja ozbiljan bezbednosni rizik jer omogućava kompromitovanje poverljivosti sistema, a u određenim scenarijima i potpunu kontrolu nad serverom.

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 9.8 (Critical)
- **Vektor:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **Objašnjenje komponenti vektora:**
  - **AV:N** (Attack Vector – Network):
    - Napad se može izvršiti udaljeno preko mreže, bez fizičkog ili lokalnog pristupa sistemu.
  - **AC:L** (Attack Complexity – Low):
    - Eksploatacija je jednostavna i ne zahteva posebne uslove ili kompleksne korake.
  - **PR:N** (Privileges Required – None):
    - Napadaču nisu potrebne nikakve privilegije ili prethodna autentifikacija.
  - **UI:N** (User Interaction – None):
    - Nije potrebna interakcija korisnika da bi se napad uspešno izvršio.
  - **S:U** (Scope – Unchanged):
    - Ranjivost utiče samo na kompromitovani Tomcat servis i ne menja bezbednosni domen drugih komponenti sistema.
  - **C:H** (Confidentiality – High):
    - Moguć je potpuni kompromis poverljivih podataka (čitanje proizvoljnih fajlova sa servera).
  - **I:H** (Integrity – High):
    - U određenim konfiguracijama moguće je menjanje sadržaja i ubacivanje zlonamernog koda.
  - **A:H** (Availability – High):
    - Postoji mogućnost narušavanja dostupnosti servisa, uključujući pad ili preuzimanje kontrole nad serverom.
- **Opravdanje:**
  Ranjivosti CVE-2020-1938 (Ghostcat) dodeljen je veoma visok CVSS skor zbog kombinacije izuzetno nepovoljnih faktora. Napad je moguće izvršiti udaljeno, bez ikakve autentifikacije ili interakcije korisnika, što značajno povećava verovatnoću uspešne eksploatacije. Uticaj ranjivosti je kritičan jer omogućava neovlašćeni pristup osetljivim fajlovima, a u određenim scenarijima i udaljeno izvršavanje koda, čime su ugroženi poverljivost, integritet i dostupnost sistema.

Dodatno, ranjivost pogađa široko korišćen serverski softver (Apache Tomcat), što povećava njen ukupni rizik i obim potencijalne zloupotrebe.

---

3. Dostupnost eksploita

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

  Da.

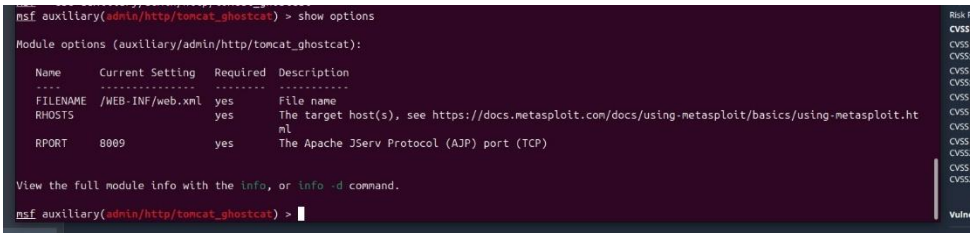
  Za ranjivost Apache Tomcat AJP Connector Request Injection (Ghostcat) postoji javno dostupan eksploit. Eksploit je dostupan u okviru Metasploit Framework-a kao pomoćni (auxiliary) modul pod nazivom: *auxiliary/admin/http/tomcat_ghostcat*. Eksploit omogućava zloupotrebu neautentifikovanog AJP konektora kako bi se izvršilo čitanje osetljivih fajlova sa servera, kao što je WEB-INF/web.xml, koji može sadržati poverljive informacije (konfiguracije, putanje, tajne). Modul cilja Apache JServ Protocol (AJP) servis koji podrazumevano radi na TCP portu 8009, i ne zahteva validne korisničke kredencijale.

- **Opis eksploita:**

  Eksploit koristi slabosti u implementaciji AJP protokola kako bi prosledio specijalno formirane zahteve Tomcat serveru. Ukoliko AJP konektor nije zaštićen autentifikacijom, napadač može da pristupi internim resursima aplikacije, što može predstavljati osnovu za dalje napade, uključujući potencijalnu eskalaciju do daljinskog izvršavanja koda (RCE)

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

  Eksploit je javno dostupan u Metasploit Framework-u, a srž eksploita se sastoji u slanju prilagođenih AJP zahteva ka ciljanom serveru. Screenshot korišćenog Metasploit modula i njegovih opcija priložen je kao dokaz dostupnosti eksploita.



---

4. Analiza uzroka (root cause)

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

  Ranjivost Apache Tomcat AJP Connector Request Injection (Ghostcat) uvedena je zbog nebezbedne podrazumevane konfiguracije AJP konektora u Apache Tomcat serveru. Konkretno, AJP konektor (Apache JServ Protocol), koji se koristi za komunikaciju između web servera i Tomcat aplikacionog servera, nije zahtevao autentifikaciju niti adekvatnu validaciju zahteva koji mu se prosleđuju.

- Problem je prisutan u više verzija Apache Tomcat servera pre zakrpe objavljene 2020. godine, uključujući verzije:

  - 7.x pre 7.0.100
  - 8.5.x pre 8.5.51
  - 9.0.x pre 9.0.31

  Zbog nedostatka kontrole pristupa i validacije AJP zahteva, napadač je mogao da šalje specijalno formirane AJP poruke koje omogućavaju čitanje internih fajlova aplikacije, kao što je WEB-INF/web.xml. Ovi fajlovi nisu predviđeni za direktan pristup spolja, ali su kroz ranjivi AJP konektor postajali dostupni.

- Root cause ove ranjivosti može se opisati kao:

  - neadekvatna validacija ulaznih AJP zahteva,
  - implicitno poverenje u internu mrežnu komunikaciju,
  - izostanak autentifikacije na AJP konektoru u podrazumevanoj konfiguraciji.

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

  U ovom slučaju, ranjivost nije posledica jedne konkretne linije aplikacionog koda, već dizajnerske i konfiguracione greške u implementaciji AJP protokola unutar Apache Tomcat servera. Eksploit koristi način na koji Tomcat obrađuje AJP zahteve, a ne grešku u poslovnoj logici aplikacije. Zbog toga se primer koda odnosi na formatiranje AJP zahteva koji omogućavaju pristup internim resursima, što je demonstrirano kroz javno dostupne alate i Metasploit module, a ne kroz izvorni kod aplikacije.

---

5. Preporuke za mitigaciju

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

  Da. Apache Software Foundation je objavila zvanične zakrpe za ranjivost Ghostcat (CVE-2020-1938 / CVE-2020-1745)**.** Problem je rešen u sledećim verzijama Apache Tomcat servera:
  - Apache Tomcat 7.0.100
  - Apache Tomcat 8.5.51
  - Apache Tomcat 9.0.31

- **Mitigation Strategy:**

  Najefikasnija i preporučena strategija mitigacije je ažuriranje Apache Tomcat servera na verziju koja sadrži bezbednosne ispravke. Nakon nadogradnje, AJP konektor više nije podrazumevano izložen bez autentifikacije.
- Konkretni koraci mitigacije uključuju:
  - nadogradnju Tomcat servera na zvanično ispravljenu verziju,
  - proveru i ograničavanje izloženosti AJP konektora isključivo na internu mrežu,
  - eksplicitno omogućavanje autentifikacije za AJP konektor (secretRequired="true"),
  - restartovanje servisa nakon primene izmene.
- Primena zakrpa može se izvršiti manuelno ili automatizovano korišćenjem alata za upravljanje paketima i konfiguracijom, kao što su:
  - apt / yum (u zavisnosti od distribucije),
  - Ansible, Puppet ili Chef u automatizovanim okruženjima,
  - CI/CD pipeline mehanizmi u produkcionim sistemima.

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

  U slučaju da nadogradnja servera nije odmah moguća, mogu se primeniti privremene mere zaštite, koje značajno smanjuju rizik eksploatacije:
  - potpuno onemogućavanje AJP konektora ako nije neophodan za rad sistema,
  - ograničavanje pristupa AJP portu (podrazumevano 8009) putem firewall pravila,
  - vezivanje AJP konektora isključivo za localhost,
  - filtriranje AJP saobraćaja na mrežnom nivou.

  Ove mere predstavljaju privremenu mitigaciju, ali se ne smatraju trajnim rešenjem – preporučuje se primena zvaničnog vendor patch-a čim to bude moguće.