Vulnerability Assessment Report Template

Very Secure FTP Daemon - vsftpd 2.3.4 Backdoor

**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-2011-2523**
* **Opis:**
* Ova ranjivost se odnosi na backdoor u vsftpd verziji 2.3.4 koja ga sadrzi na jednom od popularnih FTP servera. Ova ranjivost se javlja zbog namerno ubacenog backdoor koda gde je autentikacija uspesna ako napadac unese specificno korisnicko ime. Ranjivost moze da omogući napadaču koji koristi FTP klijent ili Netcat za povezivanje sa serverom I koji uspe da se poveže na FTP port (21/TCP) da iskoristi specifičan backdoor ako se pritom koristi i specifična kombinacija korisničkog imena. Kada se backdoor aktivira, napadač može da dobije pristup komandnoj liniji sa root privilegijama.

Ova ranjivost cilja FTP servis na portu 21 preko protokola TCP.

### **2. CVSS skor**

* **CVSS skor (numerička vrednost):** **7.5**

**Vektor:** 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): Ranjivost se može iskoristiti preko mreže.
* AC (Attack Complexity): L (Low): Eksploatacija zahteva jednostavne korake i dostupna je kroz jednostavno povezivanje na FTP server.
* PR (Privileges Required): N (None): Napadač zapravo i ne mora imati nikakve privilegije da bi iskoristio ovu konkretnu ranjivost.
* UI (User Interaction): N (None): Nije potrebna apsolutno nikakva interakcija korisnika da bi se aktivirala ranjivost.
* S (Scope): U (Unchanged): Eksploatacija ne menja privilegije napadača izvan ranjivog sistema.
* C (Confidentiality): H (High): Uspešna eksploatacija omogućava napadaču root pristup time ugrožavajući poverljivost podataka.
* I (Integrity): H (High): Integritet sistema je značajno ugrožen, Samim tim sto napadač može menjati podatke.
* A (Availability): H (High): Dostupnost sistema može biti narušena jer je moguća zloupotreba resursa.

**Opravdanje:**

Ovaj CVSS skor je dodeljen jer je ranjivost lako iskoristiva preko mreže, omogućava znacajno visok nivo privilegija bez prethodne autentifikacije, zatim i ugrožavanje poverljivosti, potom i integritet ali i dostupnost 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.

**Javno dostupan eksploat:**

* + **Exploit-DB:** Exploit-DB 17491 - Eksploit za backdoor u vsftpd verziji 2.3.4.
  + **GitHub:** Moze se pronaći kao jednostavni primeri shell skripti na GitHubu ali specifične implementacije moguce da neće biti obuhvaćene.
* **Opis eksploita:**Ako postoji eksploit, navedite detalje o tome kako funkcioniše, šta cilja, i koje su potencijalne posledice uspešnog napada.

Eksploatacija ove ranjivosti zahteva povezivanje na FTP server i korišćenje username-a sa smile-om (":)") kao deo username-a.

Kada se ovo korisničko ime unese, FTP server aktivira backdoor i otvara komandnu liniju na portu 6200, time omogućavajući napadaču pristup kao root korisnik.

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

# Eksploatacija backdoor-a se moze izvrsiti sledecim koracima

nc <ip\_adresa> 21

USER testuser:)

PASS password

nc <ip\_adresa> 6200

Nakon ovoga biće otvoren pristup komandnoj liniji na portu 6200.

### **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").

Ranjivost je uvedena u vsftpd verziji 2.3.4 kroz kod koji sadrži u sebi backdoor mehanizam. Ovo nije greška nego namerno ugrađen backdoor, da bi se kasnije otkrilo da predstavlja ozbiljan sigurnosni rizik.

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

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

Konkretan primer nije direktno dostupan, ali se zna da je kod backdoor-a deo izvršnog file-a verzije 2.3.4.

### **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…

Update vsftpd na verziju 2.3.5 ili noviju, gde je backdoor uklonjen.

Preporučuje se korišćenje alata za upravljanje paketima (apt-get upgrade) kako bi se primenila najnovija verzija.

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

Opis kako bi se ovo moglo rešiti dobudživanjem trenutne verzije

Ako ažuriranje nije moguće, trebao bi da se ogranici pristup FTP portu sa specifičnih IP adresa kroz firewall pravila dok se ne pronađe neko trajnije rešenje.