Vulnerability Assessment Report Template

Ime i prezime: Biljana Mijić
Tim: 11
Datum: 27.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID: CVE-2014-0226**

- **Opis:**
  Ova ranjivost utiče na *mod_status* modul u Apache HTTP serveru, gde postoji race condition u obradi tzv. scoreboard-a. Scoreboard je struktura podataka koju koristi Apache da prati status svakog procesa koji obrađuje zahteve. Usled ovog race condition-a, daljinski napadač može izazvati situaciju u kojoj dolazi do nesinhronizovanog pristupa ovim podacima, što može dovesti do:

    - **Izvršavanja proizvoljnog koda:** Napadač može potencijalno iskoristiti ovaj nesinhronizovani pristup za izvršenje proizvoljnog koda na serveru, što bi moglo omogućiti preuzimanje kontrole nad serverom

    - **Pristupa poverljivim informacijama:** Nesinhronizovani pristup može omogućiti napadaču da vidi osetljive podatke iz radne memorije, uključujući informacije o korisničkim sesijama, IP adresama, ili osetljive podatke kao što su kredencijali iz .htaccess fajlova

    - **Denial of Service (DoS):** Napadač može izazvati preopterećenje scoreboard-a I resursa servera, ometajući njegovo normalno funkcionisanje I onemogućavajući drugim korisnicima pristup.

  Servis: Apache HTTP server
  Port: 80(HTTP) ili 443(HTTPS), zavisno od konfiguracije

  Protokol: HTTP

2. CVSS skor

- **CVSS skor (numerička vrednost): 7.3**
- **Vektor: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L**
  Objašnjenje CVSS vektora:
  - AV (Attack Vector): N (Network) – Eksploatacija se može dogoditi preko mreže kao što je internet
  - AC (Attack Complexity) – L (Low) – Eksploatacija je relativno jednostavna jer ne zahteva složene uslove i mnogo tehničkog znanja
  - PR (Privileges Required): N (None) – Napadaču nisu potrebna posebna prava pristupa ili nalog za uspešnu eksploataciju
  - UI (User Interaction): N (None) – Nije potrebna interakcija korisnika tako da napad može biti automatski
  - S (Scope) : U (Unchanged) – Eksploatacija ne utiče na druge komponente van servera, opseg ranjivosti nije promenjen
  - C (Confidentiality Impact) – L (Low) – Napadač ima delimičan pristup informacijama i nema kontrolu nad tim čemu može pristupiti, tako da postoji mogućnost da pristupi nekim osetljivim informacijama
  - I (Integrity Impact): L (Low) – Ograničena količina informacije može biti promenjena ili modifikovana
  - A (Availability Impact): L (Low) – Dostupnost može biti povremeno ograničena, ili uspešan napad može negativno uticati na performanse, postoji mogućnost obaranja sistema I iscrpljivanja resursa
- **Opravdanje:**

  Ova ranjivost ima CVSS skor 7.3 jer je lako eksploatabilna (mrežni napad bez autentifikacije ili korisničke interakcije) I može dovesti do narušavanja poverljivosti, integriteta I dostupnosti, iako u ograničenom obimu. Mala kompleksnost napada značajno povećava rizik. Međutim, uticaj je ograničen samo na ranjivu komponentu, napadač može ostvariti samo delimičan pristup informacijama I delimičnu modifikaciju podataka, bez širih efekata na druge sisteme.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**

  Postoji javno dostupan exploit vezan za ovu ranjivost:
  https://www.exploit-db.com/exploits/34133

- **Opis eksploita:**
  Eksploit ove ranjivosti se odnosi na *race-condition* izmedju *scoreboard*-a HTTPD-a I *mod_status*-a.
  Eksploit funkcioniše tako što napadač pokreće HTTPD server sa aktivnim *mod-status*-om koji pruža informacije o trenutnim vezama i stanju servera. Napadač dalje koristi tehnike koje omogućavaju simultani pristup *mod-status*-u I *scoreboard*-u, čime se izaziva race condition u sistemu. Ovo se može sprovesti slanjem više HTTP zahteva u veoma kratkom vremenskom periodu. U slučaju uspešnog napada, dolazi do prelivanja bafera u memoriji, što omogućava napadaču da preuzme kontrolu nad memorijskim segmentima i može otkriti sadržaj iz drugih delova memorije. Na taj način može doći do curenja privatnih informacija, i napadač može pristupiti podacima kao što su kredencijali iz *.htaccess* fajlova, privatni ključevi SSL sertifikata, i druge osetljive informacije.

- **Kod eksploita (ukoliko postoji):**

  Glavne dve funkcije koda eksploita su prikazane na slikama:

```
    1908AP_DECLARE(char *) ap_escape_logitem(apr_pool_t *p, const char
*str)
    1909{
    1910    char *ret;
    1911    unsigned char *d;
    1912    const unsigned char *s;
    1913    apr_size_t length, escapes = 0;
    1914
    1915    if (!str) {
    1916        return NULL;
    1917    }
    1918
    1919    /* Compute how many characters need to be escaped */
    1920    s = (const unsigned char *)str;
    1921    for (; *s; ++s) {
    1922        if (TEST_CHAR(*s, T_ESCAPE_LOGITEM)) {
    1923            escapes++;
    1924        }
    1925    }
    1926
    1927    /* Compute the length of the input string, including NULL
*/
    1928    length = s - (const unsigned char *)str + 1;
    1929
    1930    /* Fast path: nothing to escape */
    1931    if (escapes == 0) {
    1932        return apr_pmemdup(p, str, length);
    1933    }
```

```
       112APR_DECLARE(void *) apr_pmemdup(apr_pool_t *a, const void
*m, apr_size_t n)
       113{
       114    void *res;
       115
       116    if (m == NULL)
       117      return NULL;
       118    res = apr_palloc(a, n);
       119    memcpy(res, m, n);
       120    return res;
```

Na prvoj slici je prikazana funkcija *ap_escape_logitem* koja prima string I vrši obradu stringa kako bi izbegla određene specijalne karaktere, tj. one koji mogu biti opasni u zapisima logova. Prvi deo funkcije računa dužinu stringa *str* I prebrojava karaktere koje treba izbeći. Na osnovu toga, funkcija određuje veličinu memorijskog prostora potrebnog za kopiranje obrađenog stringa.

Funkcija *apr_memdup* koristi se za kopiranje podataka u novododeljenu memorijsku lokaciju.

Problem može nastati jer funkcija *ap_escape_logitem* može da se koristi u više niti istovremeno u *mod_status* modulu Apache servera. Svaka nit može pristupiti ili menjati scoreboard u isto vreme. Zahtev koji se obrađuje može biti istovremeno pristupan od strane više niti, što znači da jedna nit može čitati ili kopirati podatke dok druga menja njihov sadržaj.

Scenario napada se može sprovesti tako što jedna nit može pozvati *ap_escape_logitem(pool, ws_record->request)* gde je *ws_record->request* inicijalno prazan string, dok u međuvremenu druga nit može izmeniti sadržaj *ws_record->request* u na primer “GET / HTTP/1.0”.

Kao rezultat, *apr_memdup* funkcija može kopirati samo prvi bajt iz novog sadržaja (na primer, “G”), dok preostali deo memorije ostaje sa nasumičnim podacima. To može dovesti do:

- Preliva memorije (Heap Overflow): Nedostatak \0 na kraju može izazvati nepravilan završetak stringa, što može dovesti do curenja u memoriji
- Otkrivanja osetljivih informacija: String sada može sadržavati nasumične podatke iz memorije, što može uključiti osetljive podatke poput korisničkih sesija ili privatnih ključeva
- DoS napada: Kopiranje nasumičnih vrednosti može dovesti do iscrpljivanja memorijskih resursa, izazivajući pad sistema

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  Ranjivost je uvedena u ranijim verzijama Apache HTTP servera pre verzije 2.2.28. i prisutna je u verzijama od 2.2.0 do 2.2.27, kao I u određenim verzijama iz serije 2.4, uključujući 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, i 2.4.1.. Greška je posledica neadekvatnog rukovanja višestrukim paralelnim zahtevima u *scoreboard*-u *mod_status* modula, što omogućava napadaču da izazove race condition.

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

  Nema javno dostupnog primera koda za ovu grešku, ali root cause se nalazi u neadekvatnoj sinhronizaciji *scoreboard*-a prilikom rukovanja konkurentnim pristupima. Ova greška omogućava različitim zahtevima da pristupe memorijskom delu koji koristi *mod_status* što vodi ka race condition situacijama.

---

5. Preporuke za mitigaciju

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

  Apache je objavio patch za ovu ranjivost u verziji 2.2.28, koja ispravlja race condition problem u *mod_status*-u. Kao mera mitigacije, preporučuje se ažuriranje Apache servera na verziju 2.2.28 ili noviju.

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

  Ako ažuriranje na noviju verziju nije moguće, rešenje je da se ograniči pristup *mod_status* stranici samo na interne IP adrese. Takođe se preporučuje I konfiguracija Apache servera tako da *mod_status* koristi *ExtendedStatus Off* kako bi smanjio količinu informacija dostupnih na stranici statusa, čime se donekle smanjuje potencijalni uticaj ranjivosti.