Vulnerability Assessment Report Template (1)

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.

  Komande za ažuriranje:

  1. Ažuriranje liste paketa: sudo apt-get update
  2. Ažuriranje Apache servera: sudo apt-get install apache2
  3. Restartovanje Apache servisa: sudo systemctl restart apache2

- **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.

Vulnerability Assessment Report Template (2)

Ime i prezime: Biljana Mijić
Tim: 11
Datum: 1.11.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

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

- **Opis:**
  "Terrapin Prefix Truncation Weakness" predstavlja ranjivost u određenim SSH serverima koja omogućava napadaču u sredini (MITM – man-in-the-middle) da oslabi proveru integriteta SSH veze I eventualno smanji sigurnost same veze. Ova ranjivost pogađa SSH servere koji koriste algoritme enkripcije ChaCha20-Poly1305 I CBC sa Encrypt-then-MAC.
    - **Servis:** SSH (Secure Shell)
    - **Port**: 22
    - **Protokol**: TCP

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 5.9**
- **Vektor:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
    - **AV (Attack Vector): N (Network) –** Eksploatacija se može dogoditi preko mreže, kao što je internet
    - **AC (Attack Complexity): H (High) –** Napad je složen I zahteva posebne uslove ili specijalizovano znanje da bi se uspešno izvršio
    - **PR (Privileges Required): N (None) –** Napadač ne mora imati nikakve privilegije, može iskoristiti ranjivost kao običan korisnik ili čak anonimni napadač
    - **UI (User Interaction): N (None) –** Nije potrebna interakcija korisnika za uspešan napad
    - **S (Scope): U (Unchanged) –** Eksploatacija ne utiče na druge komponente van servera, opseg ranjivosti nije promenjen

- **C (Confidentiality Impact): N (None) –** Nema uticaja na poverljivost, napad ne dovodi do otkrivanja tajnih informacija
- **I (Integrity Impact): H (High) –** Postoji visok uticaj na integritet, napad može dovesti do neautorizovanih izmena podataka
- **A (Availiability Impact): N (None) –** Nema uticaja na dostupnost, napad ne dovodi do prekida rada sistema ili usluga

- **Opravdanje:**

  Ova ranjivost ima CVSS skor 5.9 što predstavlja umeren rizik, jer je verovatnoća da će se ovaj napad desiti relativno mala. Iako je eksploatabilan putem mreže I nisu potrebne dodatne privilegije napadača, kao ni interakcija korisnika, napad je složen I zahteva visoko tehničko znanje napadača da bi ga izveo. Iako ne utiče na poverljivost I dostupnost, postoji visok uticaj na integritet, što znači da napadać može izvršiti neautorizovane izmene podataka, dok opseg ranjivosti ostaje nepromenjen I utiče samo na lokalni sistem.

---

3. Dostupnost eksploita

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

  Ne postoje javno dostupni eksploiti za ovaj CVE ali postoji git repozitorijum koji prikazuje dokaz koncepta (Proof of Concept) koji se odnosi na ovu ranjivost:

  https://github.com/RUB-NDS/Terrapin-Artifacts/blob/main/scripts/test-ext-downgrade.sh

- **Opis eksploita:**

  Ovaj eksploit se odnosi na napad tipa “extension downgrade” koji cilja na sigurnost SSH veze između klijenta I servera. Kroz korišćenje posredničkog servera (proxy), napadač preusmerava komunikaciju omogućavajući man-in-the-middle (MITM) napad. Cilj napada je da prisili klijent i server da koriste slabije kriptografske algoritme ili verzije protokola, čime se smanjuje nivo sigurnosti veze. Umesto savremenih i sigurnijih opcija, napadač može usmeriti komunikaciju na ranije verzije kriptografskih algoritama koje su poznate po slabostima u pogledu sigurnosti. Na taj način napadač može da presretne i potencijalno dešifruje poverljive informacije koje se razmenjuju tokom komunikacije.

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

  Na repozitorijumu je dostupna bash skripta koja služi za simulaciju više servera putem Docker kontejnera. Skripta se koristi za demonstraciju eksploatacije ranjivosti u SSH

protokolu kroz napad poznat kao "downgrade attack". Kada se pokrene, skripta pokreće Docker kontejnere koji predstavljaju klijente I servere, kao I proxy server koji usmerava sav saobraćaj između njih. Ovaj proxy može manipulisati podacima, tako da obezbeđuje da se komunikacija vrši koristeći ranjive enkripcijske metode, kao što su ChaCha20-Poly1305 ili različite varijante CBC-EtM. Na taj način napadač može da presretne I potencijalno dešifruje podatke koji se razmenjuju. Na slici je prikazana funkcija *select_and_run_poc_proxy* koja omogućava korisniku da odabere specifičnu varijantu napada I pokrene odgovarajući proxy server.

```
105  function select_and_run_poc_proxy {
106    echo "[i] This script supports the following extension downgrade attack variants as PoC:"
107    echo -e "\t1) ChaCha20-Poly1305"
108    echo -e "\t2) CBC-EtM (Unknown)"
109    echo -e "\t3) CBC-EtM (Ping)"
110    read -p "[+] Please select PoC variant to test [1-3]: " POC_VARIANT
111
112    case $POC_VARIANT in
113      1)
114        POC_VARIANT_NAME="ChaCha20-Poly1305"
115        POC_IMAGE="terrapin-artifacts/ext-downgrade-chacha20-poly1305" ;;
116      2)
117        POC_VARIANT_NAME="CBC-EtM (Unknown)"
118        POC_IMAGE="terrapin-artifacts/ext-downgrade-cbc-unknown" ;;
119      3)
120        if [[ $SERVER_IMPL -eq 2 ]]; then
121          echo "[!] CBC-EtM (Ping) variant requires OpenSSH 9.5p1 as the server. Please re-run the script."
122          exit 1
123        fi
124        POC_VARIANT_NAME="CBC-EtM (Ping)"
125        POC_IMAGE="terrapin-artifacts/ext-downgrade-cbc-ping" ;;
126      *)
127        echo "[!] Invalid selection, please re-run the script"
128        exit 1 ;;
129    esac
130    echo "[+] Selected PoC variant: '$POC_VARIANT_NAME'"
131
132    echo "[+] Starting extension downgrade attack proxy on port $POC_PORT. Connection will be proxied to 127.0.0.1:$SERVER_PORT"
133    docker run -d \
134      --network host \
135      --name $POC_CONTAINER_NAME \
136      $POC_IMAGE --proxy-port $POC_PORT --server-ip "127.0.0.1" --server-port $SERVER_PORT > /dev/null 2>&1
137  }
```

---

4. Analiza uzroka (root cause)

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

  Ranjivost CVE-2023-48795 prouzrokovana je problemom u SSH Binary Packet Protocol (BPP), koji je implementiran kroz određene ekstenzije. U fazi uspostavljanja veze dolazi do nepravilnog rukovanja sekvencijalnim brojevima, što omogućava efektivne napade na korišćenje **ChaCha20-Poly1305** enkripcije (kao i na CBC sa Encrypt-then-MAC). Ova ranjivost se pojavila zbog neadekvatne validacije tokom handshake veze, što omogućava napadačima da zaobiđu bezbedonosne mehanizme.

Ovaj problem je posebno uticao na različite verzije OpenSSH, kao I na brojne druge SSH implementacije, uključujući Maverick Synergy Java SSH API, Dropbear, PuTTY, AsyncSSH i druge.

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

  Nema javno dostupnog primera koda za ovu grešku, ali jedan od ključnih problema je neadekvatna obrada sekvencijalnih brojeva tokom faze rukovanja u SSH protokolu. Na primer, deo koda koji se odnosi na rukovanje paketima može sadržati logiku koja ne validira ispravnost sekvencijalnih brojeva, što omogućava napadaču da preskoči određene brojeve I izazove neusaglašenost u komunikaciji.

---

5. Preporuke za mitigaciju

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

  Ažuriranje verzije – prvo se preporučuje ažuriranje verzije na najnoviju verziju koja sadrži ispravke za ovu ranjivost. Nakon ažuriranja, treba proveriti da li klijent I server podržavaju nove *kex* (key exchange) pseudo-algoritme koji osiguravaju zaštitu od napada. Ako klijent pruža kex-strict-c-v00@openssh.com a server odgovara sa kex-strict-s-v00@openssh.com, nema potrebe za daljim koracima.

  Komanda za ažuriranje na RHEL sistemima: sudo dnf update openssh

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

  Onemogućavanje slabih šifri – ako se pomenuti algoritmi ne nalaze u odgovoru, mogu se privremeno onemogućiti određene šifre I HMAC-ovi kao alternativno rešenje. Lista šifri koje treba onemogućiti :

    - chacha20-poly1305@openssh.com
    - hmac-sha2-512-etm@openssh.com
    - hmac-sha2-256-etm@openssh.com
    - hmac-sha1-etm@openssh.com
    - hmac-md5-etm@openssh.com

  Ove promene se mogu primeniti putem crypto-policies tako što se kreira podpolitika. Može se kreirati */etc/crypto-policies/policies/modules/CVE-2023-48795.pmod* datoteka sa sledećim linijama (java):

  cipher@SSH = -CHACHA20-POLY1305

  ssh_etm = 0,

I zatim da se pokrene komanda (ruby):

```
update-crypto-policies --set $(update-crypto-policies --show):CVE-2023-48795
```

Nakon toga treba da se restartuje OpenSSH server.

Vulnerability Assessment Report Template (3)

Ime i prezime: Biljana Mijić
Tim: 11
Datum: 2.11.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID: CVE-2017-1000028**
- **Opis:**

  CVE-2017-1000028 je *Directory Traversal* ranjivost koja utiče na Oracle GlassFish Server Open Source Edition 4.1. Ranjivost omogućava napadačima da pristupe fajlovima na serveru koji inače ne bi trebalo da budu dostupni. Ranjivost postoji zbog nepravilnog rukovanja HTTP GET zahtevima u GlassFish Serveru, što omogućava napadaču da manipuliše putanjom fajla. Napadač može, bez autentifikacije, pristupiti fajlovima sa osetljivim informacijama, što može dovesti do krađe podataka ili daljih napada na sistem.

  - **Servis:** Oracle GlassFish Server Open Source Edition
  - **Port**: 4848
  - **Protokol**: TCP

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 7.5**
- **Vektor: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N**

    - **AV (Attack Vector): N (Network) –** Eksploatacija se može dogoditi preko mreže, kao što je internet
    - **AC (Attack Complexity): L (Low) –** Kompleksnost napada je niska, napadaču nisu potrebne specijalizovane tehnike ili dodatni uslovi za uspešan napad
    - **PR (Privileges Required): N (None) –** Napadač ne mora imati nikakve privilegije, može iskoristiti ranjivost kao običan korisnik ili čak anonimni napadač
    - **UI (User Interaction): N (None) –** Nije potrebna interakcija korisnika za uspešan napad
    - **S (Scope): U (Unchanged) –** Eksploatacija ne utiče na druge komponente van servera, opseg ranjivosti nije promenjen
    - **C (Confidentiality Impact): H (High) –** Uspešno iskorišćavanje ove ranjivosti može dovesti do potpunog kompromitovanja poverljivih podataka na sistemu
    - **I (Integrity Impact): N (None) –** Nema uticaja na integritet podataka. Napadač ne može modifikovati podatke na serveru koristeći ovu ranjivost.
    - **A (Availiability Impact): N (None) –** Eksploatacija ranjivosti ne utiče na dostupnost servisa, tako da sistem neće biti zaustavljen ili usporen.
- **Opravdanje:**
  Ova ranjivost ima visok CVSS skor jer je vrlo lako eksploatabilna I ima značajan uticaj na poverljivost sistema. Napad se može izvršiti preko mreže i ne zahteva visoku tehničku složenost. Ne zahtevaju se nikakve privilegije niti korisnička interakcija, što omogućava anonimnim napadačima da iskoriste ranjivost samostalno. Iako napad ne utiče na integritet ni dostupnost sistema, ugrožava poverljivost, omogućavajući pristup osetljivim podacima na serveru. Obim ranjivosti je nepromenjen i ostaje ograničen na lokalni sistem, ali ozbiljan uticaj na poverljivost opravdava visoki rizik koji ovaj CVSS skor predstavlja.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Postoji javno dostupan exploit (nije verifikovan): https://www.exploit-db.com/exploits/45198
- **Opis eksploita:**
  Ovaj exploit iskorišćava *directory traversal* ranjivost u Oracle GlassFish Open Source Edition 4.1, koja se nalazi u administrativnoj konzoli. Napad se izvršava slanjem

posebno oblikovanog HTTP GET zahteva na server, koji omogućava napadaču da navigira kroz strukturu direktorijuma na serveru.
Konkretno, exploit koristi kodiranu sekvencu *%c0%af..* , koja predstavlja *../* u URL-u. Ova sekvenca omogućava napadaču da se "vrati" u prethodne direktorijume. Koristeći ovaj mehanizam, napadač može pristupiti fajlovima izvan predviđenih direktorijuma aplikacije tako što će precizirati putanju do željenog fajla putem opcije *FILEPATH.* Na primer, napadač može da preuzme fajlove kao što su konfiguracione datoteke, koje često sadrže osetljive informacije. Na ovaj način, napadač može da pristupi osetljivim informacijama na serveru.

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

```
def run_host(ip)
  filename = datastore['FILEPATH']
  traversal = "%c0%af.." * datastore['DEPTH'] << filename

  res = send_request_raw({
    'method' => 'GET',
    'uri'    => "/theme/META-INF/prototype#{traversal}"
  })

  unless res && res.code == 200
    print_error('Nothing was downloaded')
    return
  end

  vprint_good("#{peer} - #{res.body}")
  path = store_loot(
    'oracle.traversal',
    'text/plain',
    ip,
    res.body,
    filename
  )
  print_good("File saved in: #{path}")
end
```

U ovoj funkciji se postavlja logika za izvođenje napada.

- filename: Uzima vrednost iz prethodno registrovane opcije FILEPATH, gde se definiše putanja koja se želi pročitati
- traversal: Generiše string koji se koristi za directory traversal, koristeći kodirane sekvence koje predstavljaju “../” (sekvenca “%c0%af..” predstavlja kodiranu verziju “../” u URL-encoded formatu) . Ovo se ponavlja DEPTH puta (dubina za directory traversal koju je korisnik prethodno postavio), što omogućava napadaču da navigira kroz strukturu direktorijuma.

- send_request_raw: Ovaj metod šalje HTTP GET zahtev ka serveru, ciljajući URI koji je formiran da iskoristi ranjivost

Na kraju ukoliko je odgovor servera uspešan, funkcija ispisuje sadržaj preuzetog fajla I čuva ga lokalno.

---

4. Analiza uzroka (root cause)

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

  Ova ranjivost objavljena je 16. maja 2016. godine. Uzrok ranjivosti CVE-2017-1000028 leži u nedovoljnom validiranju I filtriranju korisničkog unosa koji se koristi za formiranje putanja do datoteka na serveru. U Oracle GlassFish Server Open Source Edition 4.1, administrativni interfejs nije ispravno konfigurisao pristup resursima, što omogućava napadaču da koristi tehnike directory traversal.

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

  Nema javno dostupnog primera koda za ovu ranjivost, ali uzrok ranjivosti je u nedovoljnom validiranju I filtriranju korisničkog unosa, što omogućava napadaču da koristi tehnike directory traversal I pristupi osetljivim datotekama.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
- **Mitigation Strategy:**
  Oracle je izdao patch za ranjivost CVE-2017-1000028 u okviru ažuriranja za GlassFish Server Open Source Edition 4.1. Da bi se primenio ovaj fix, korisnici bi trebali da preuzmu najnoviju verziju softvera sa zvaničnog Oracle sajta.

  Koraci:

  1. Zaustavljanje GlassFish servera komandom: asadmin stop-domain domain1 (zameniti domain1 imenom odgovarajućeg domena)
  2. Preuzeti vendor patch sa zvaničnog Oracle sajta I primeniti ga u direktorijumu u gde je instaliran GlassFish Server
  3. Ponovo pokrenuti GlassFish server komandom: asadmin start-domain domain1

  Za automatizaciju ovog procesa preporučuje se korišćenje alata kao što su Ansible, Puppet, Chef, koji mogu olakšati I ubrzati primenu patch-a.

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

Ako vendor fix nije dostupan, korisnici mogu da implementiraju dodatne mere sigurnosti, ako što su:

- Konfiguracija firewall-a kako bi se ograničio pristup administrativnom interfejsu na samo pouzdane IP adrese
- Uvođenje reverse proxy rešenja koje može dodatno filtrirati HTTP zahteve i blokirati potencijalno maliciozne unose
- Upotreba aplikacionih firewall rešenja koja mogu detektovati i blokirati napade bazirane na directory traversal tehnikama