Vulnerability Assessment Report Template

Ime i prezime: Teodor Vidaković
Tim: 1
Datum: 28.11.2025.
Scan Tool: Nessus (10.10.1 (#10) LINUX)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID: CVE-2001-0731**

- **Opis:**
  Apache HTTP Server verzije 1.3.20 sadrži ranjivost u Multiviews modulu kada je ovaj modul omogućen. Ranjivost dozvoljava udaljenom napadaču da preusmeri zahteve sa specijalno oblikovanim query stringovima oblika “M=D" da bi zaobišao index stranicu i pristupio listi sadržaja direktorijuma, čak i kada je index datoteka prisutna. Apache HTTP server sluša na standardnom HTTP 80 portu koristeći TCP protokol. Ovo predstavlja curenje informacija i može pomoći u daljoj eskalaciji napada, iako direktno ne utiče na integritet i dostupnost servisa. Link

  Multiviews modul koristi query string parametre za Content Negotiation, koji predstavlja proces odabira odgovarajućeg tipa sadržaja koji će biti vraćen klijentu. Parametri M=A, M=D, M=S omogućavaju klijentu da zahteva specifičan redosled sortiranja direktorijuma. Problem je što Apache nije adekvatno proveravao da li je prikazivanje liste direktorijuma dozvoljeno pre nego što je primenio ove parametre.

  - Informaciono otkrivanje: Napadač može videti kompletan sadržaj direktorijuma (ime, veličina, datum izmene)
  - Zaobilaženje sigurnosnih kontrola: Čak iako je index.html konfigurisan, direkorijumska lista se može prikazati
  - Prikupljene informacije se mogu koristiti za dalje napade (pronalaženje konfiguracionih datoteka, backup datoteka..)

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 5.3 (Medium)**
- **Vektor:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
    - AV:N (Attack Vector – Network): napad može biti izveden sa mreže, dovoljan je HTTP(S) pristup Apache Serveru
    - AC:L (Attack Complexity – Low): napad ne zahteva složene uslove, potreban je samo specifičan format URL-a
    - PR:N (Privileges Required – None): nije potrebna autentifikacija
    - UI:N (User Interaction – None): nije potrebna interakcija krajnjeg korisnika
    - S:U (Scope – Unchanged): ranjivost ne utiče na druge sisteme
    - C:L (Confidentiality Impact – Low): može doći do manjeg curenja informacija, mogu se otkriti struktura aplikacije, skripte..
    - I:N (Integrity Impact – None): integritet sistema nije ugrožen
    - A:N (Availability Impact – None): nema uticaja na dostupnost

- **Opravdanje:**
  Ova ocena je zasnovana na lakoći izvođenja napada sa mreže, bez potrebe za privilegijama ili korisničkom interakcijom, dok je uticaj ograničen na manji gubitak poverljivosti bez oštećenja integriteta sistema ili dostupnosti.

  Neke od mogućih posledica su:

    - Otkrivanje osetljivih fajlova (config, backup, .bak)
    - Identifikacija ranjivih skripti ili starih verzija aplikacija
    - Mapiranje strukture web aplikacije za dalje napade
    - Povećanje površine napada za druge eksploatacije

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da**
- **Opis eksploita:**
  Napadač šalje HTTP zahtev ka direktorijumu na Apache 1.3.20 serveru sa uključenim Multiviews, uz specifičan query string (npr. parametar sa “M=D”) koji zaobilazi index fajl i izaziva prikaz liste fajlova u tom direktorijumu. Ovo funkcioniše bez autentifikacije i može se ponoviti za više direktorijuma kako bi se mapirala struktura aplikacije. Link
- **Kod eksploita (ukoliko postoji):** `http://target-webserver/?M=D`

---

4. Analiza uzroka (root cause)

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

  Ranjivost se javlja u Apache HTTP Server verziji 1.3.20 u kombinaciji sa omogućenom opcijom Multiviews (mod_negotiation). Problem nastaje zbog načina na koji Apache bira odgovarajući resrurs za prikaz. Kada se koristi određeni query string, logika index fajla može biti zaobiđena, što dovodi do toga da server umesto index stranice prikaže listing direktorijuma. Glavni razlog je u neadekvatnoj validaciji.

  Zbog ovakvog ponašanja, server tretira zahtev kao da treba da prikaže varijantu sadržaja umesto da posluži index fajl, pa kao rezultat vraća listu fajlova u direktorijumu. Ova greška je adresirana u kasnijim verzijama.

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

  Tačni delovi koda u mod_negotiation i povezanim modulima nisu eksplicitno objavljeni, ali je dokumentovano da je problem rešen u novijim verzijama kroz promenu načina na koji se obrađuju zahtevi sa Multiviews i index direktorijumima. Link

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
- **Mitigation Strategy:**
  Ažurirati Apache HTTP Server 1.3.20 na noviju verziju u kojoj je problem sa Multiviews direktorijumima ispravljen.

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

  Pošto je vendor patch dostupan, primarna preporuka je nadogradnja.
  Ako iz nekog razloga nije moguće odmah nadograditi, privremeno onemogućiti Multiviews na direktorijumima koji sadrže osetljive fajlove ili na nivou cele virtuelne host konfiguracije.
  Ograničiti pristup osetljivim direktorijumima koristeći HTTP autentifikaciju, IP restrikcije ili firewall, kako bi se smanjila šansa da anonimni korisnici uopšte dođu do tih lokacija.
  Pored toga, može se redovno skenirati aplikacija i ručno proveravati da li se negde dobija directory listing umesto index stranice.