

Vulnerability Assessment Report Template

Ime i prezime: Anastasija Savić

Tim: 3

Datum: 02.11.2024.

Scan Tool: Nessus (10.8.3)

Test okruženje: Metasploitable3

1. Enumeracija CVE-a

- **CVE ID:** CVE-2016-2115
 - **Opis:** Ranjivost se odnosi na situacije u kojima SMB (*Server Message Block*) server ne zahteva digitalno potpisivanje poruka. Na ovaj način se omogućava MITM (*man-in-the-middle*) napad. Tokom napada, napadač može da potencijalno promeni neke podatke koji se prenose putem SMB-a (npr. izmena fajlova).
 - **Servis:** cifs (*Common Internet File System*)
 - **Port:** 445
 - **Protokol:** tcp
-

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:N/I:L/A:N
 - **AV(Attack Vector: Network)** - Ranjivost je dostupna preko mreže, što znači da napadač može da iskoristi ranjivost sa udaljene lokacije.
 - **AC(Attack Complexity: Low)** - Napadač može da iskoristi ranjivost relativno lako, bez posebnih uslova ili dodatnih koraka.
 - **PR (Privileges Required: None)** - Eksploatacija ranjivosti ne zahteva posebna ovlašćenja. Napadač može da iskoristi ranjivost bez prijave ili dodatnog pristupa sistemu, što je samim tim čini ozbiljnijom.
 - **UI (User Interaction: None)** - Eksploatacija ranjivosti ne zahteva nikakvu interakciju korisnika.
 - **S (Scope: Unchanged)** - Ranjivost utiče samo na komponente unutar istog bezbednosnog domena.

- **C (Confidentiality: None)** - Ova ranjivost ne omogućava napadaču da pristupi ili otkriva poverljive informacije.
 - **I (Integrity: Low)** - Postoji mali uticaj na integritet, što znači da napadač može da promeni podatke, ali to neće značajno kompromitovati sistem ili korisnike.
 - **A (Availability: None)** - Ranjivost ne utiče na dostupnost sistema. Sistem ostaje funkcionalan i ne doživljava pad performansi ili prekide u radu.
- **Opravdanje:** Što se tiče eksploataбилности, napad može da se izvrši sa bilo koje udaljene lokacije, preko mreže, bez posebnih dozvola i korisničkih autentifikacija. Napadač može delimično da utiče na integritet sistema. Ovaj uticaj nije kritičan, ali može da dovede do izmene podataka u sistemu ili presretanja informacija. Zbog jednostavnosti eksploatacije i mogućnosti da napadač izvrši napad sa minimalnim zahtevima, ranjivost se smatra ozbiljnom, iako njen uticaj na poverljivost i dostupnost ostaje ograničen. Rezultat je ranjivost sa srednjim cvss skorom, jer kompromitovanje integriteta može ugroziti systemske podatke ili omogućiti manipulaciju.
-

3. Dostupnost eksploita

- **Postoji javno dostupan exploit (Da/Ne):** Da
- **Opis exploita:** Napad može da se izvrši na nekoliko načina, jer nema kriptografske zaštite koja bi garantovala integritet podatka. Konkretno, u exploitu koji sam našla korišćen je *Responder* alat. Napadi se izvršavaju kod SMB servera koji ne zahtevaju digitalan potpis. Ovaj alat omogućava napadaču da presretne SMB autentifikacione podatke i preusmeri ih ka drugim resursima. Posledica uspešnog napada jeste uspešno presretanje komunikaciju između klijenta i servera.
- **Kod exploita (ukoliko postoji):** Na slici je prikazana komanda za pokretanje *Responder* alata. Ova komanda omogućava napadaču da sluša na mrežnoj interfejsu i presreće autentifikacione informacije.

Slika prikazuje protokole koje Responder koristi za "trovanje" mreže, kao i servise koje alat emulira. Zatim se pomoću komande `sudo ntlmrelayx.py -tf targets.txt -smb2support` se dobija neovlašćeni pristup i omogućuje se komunikacija sa ciljnim sistemom čija se ip adresa nalazi u *targets.txt* fajlu.


```
| smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge response: supported  
|_ message_signing: disabled (dangerous, but default)
```

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da
- **Mitigation Strategy:** Problem ove ranjivosti može da bude rešen ukoliko se ažurira Samba verzija na neku od novijih verzija (4.2.11, 4.3.8, 4.4.2). Pored toga, preporučuje se da omogući opcija `client ipc signing = required` u Samba konfiguracionom fajlu za dodatnu zaštitu. Za dodatne konfiguracije pogledati sledeći link:

<https://retest.dk/vulnerabilities-base/smb-signing-not-required/>
- **Alternativni fix (ukoliko ne postoji vendorski):**