Vulnerability Assessment Report Template

Ime i prezime: Andjela Vukosav

Tim:

Datum: 09.12.2025.

Scan Tool: Nessus (verzija)

Test okruženje: Metasploitable3

1. Enumeracija CVE-a

• CVE ID: CVE-2004-2761 (SSL Certificate Signed Using Weak Hashing Algorithm - MD5)

• Opis: Ranjivost se odnosi na upotrebu SSL/TLS sertifikata potpisanih kriptografski slabim algoritmom — konkretno, *md5WithRSAEncryption*. Ova heš funkcija (MD5) se smatra nesigurnom zbog poznatih napada kolizije, koji omogućavaju napadaču da kreira drugi sertifikat sa istim hash-om kao originalni, čime se otvara mogućnost za spoofing ili man-in-the-middle (MITM) napade. U ovom slučaju, pogođeni servis je HTTPS servis koji koristi SSL/TLS protokol na standardnom portu 443/tcp. Sertifikacioni lanac koji server prezentuje klijentima sadrži barem jedan sertifikat potpisan korišćenjem MD5 algoritma, što znači da klijenti koji se povezuju na ovaj servis potencijalno komuniciraju preko nesigurne kriptografske osnove. Ranjivost je identifikovana putem Nessus skeniranja, pomoću plugina ID 35291. Pogođena IP adresa servera je 192.168.56.101, a ranjivost je potvrđena analizom SSL sertifikata prikazanih u odgovoru skenera.

2. CVSS skor

• CVSS skor (numerička vrednost): 5.3 (Medium) – CVSS v3.0

• Vektor: ***CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N***

- ***AV:N (Attack Vector: Network):*** Napad se može izvesti daljinski putem mreže, bez fizičkog pristupa. U ovom slučaju, napadač može iskoristiti ranjivost presretanjem SSL komunikacije između klijenta i servera koristeći lažni sertifikat. .

- ***AC:L (Attack Complexity: Low):*** Eksploatacija je relativno jednostavna i ne zahtijeva složene uslove. Potrebno je samo imati pristup mreži kroz koju prolazi komunikacija (npr. WiFi, lokalna LAN mreža, ili na internetu kroz MITM).
- ***PR:N (Privileges Required: None):*** Napadaču nisu potrebne nikakve privilegije niti autentifikacija da bi iskoristio ranjivost.
- ***UI:N (User Interaction: None):*** Nije potrebna interakcija korisnika — napad se može izvesti potpuno pasivno ako napadač uspješno podmetne lažni sertifikat u sesiju.
- ***S:U (Scope: Unchanged)***: Eksploatacija ne utiče na druge komponente van ciljanog sistema – ostaje unutar okvira SSL komunikacije između servera i klijenta.
- **C:N (Confidentiality: None):** Sama ranjivost ne kompromituje direktno povjerljivost podataka. MD5 kolizija omogućava falsifikovanje sertifikata, ali ne otkrivanje već šifrovanih podataka.
- **I:L (Integrity: Low):** Napadač može kreirati lažni sertifikat koji prolazi validaciju digitalnog potpisa, čime se narušava integritet PKI (Public Key Infrastructure) sistema i omogućava spoofing identiteta servera.
- ***A:N (Availability: None):*** Nema uticaja na dostupnost – napad ne izaziva pad sistema, niti ga onemogućava.

• **Opravdanje:** Ranjivost CVE-2004-2761 omogućava napadaču da kreira falsifikovan SSL/TLS sertifikat korišćenjem MD5 collision napada. Primarni impact je na integritet autentifikacije - napadač može stvoriti lažni sertifikat koji izgleda legitimno i prolazi kriptografsku validaciju. Ovo može biti iskorišćeno za Man-in-the-Middle (MITM) napade gdje napadač imitira legitimni server. Iako MITM napad može sekundarno dovesti do gubitka povjerljivosti, direktan impact CVE-2004-2761 je na integritet PKI sistema, ne na povjerljivost komunikacije. CVSS skor je 5.3 (Medium).

3. Dostupnost eksploita

• **Postoji javno dostupan eksploit (Da/Ne):** Da.

• **Opis eksploita:** Za ranjivost CVE-2004-2761 dostupni su brojni javni resursi i demonstracije koje prikazuju kako se SSL sertifikati potpisani MD5 algoritmom mogu iskoristiti za napade kolizije, koji vode ka imitaciji (spoofing) sertifikata i Man-in-the-Middle (MITM) napadima. Najpoznatiji praktični eksploat izveden je 2008. godine od strane istraživača sa timova kao što su CWI (Amsterdam) i EPFL, koji su uspješno:

- generisali par sertifikata sa istim MD5 hash-om (kolizija),
- koristili važeći MD5 potpis od legitimnog CA za "neškodljivi" CSR (Certificate Signing Request),
- a zatim zamijenili sadržaj sertifikata zlonamjernim (npr. lažni CA),

- ❖ čime su mogli izdavati sertifikate drugim domenima i glumiti bilo koji sajt.

• **Kod eksploita (ukoliko postoji):** Srž eksploita kod ranjivosti CVE-2004-2761 je u tome da se generišu dva različita sertifikata (legitimni i zlonamjerni) koji imaju identičan MD5 hash (kolizija). Zatim se koristi potpis legitimnog sertifikata koji je izdao CA, ali se njegov sadržaj zamjenjuje zlonamjernim sadržajem. Time napadač dobija sertifikat koji izgleda potpuno validno i koji browser prepoznaje kao pouzdan, čime se omogućava MITM napad.

4. Analiza uzroka (root cause)

• **Uvođenje Greške (Commit/Verzija):** Ranjivost CVE-2004-2761 rezultat je dugogodišnje upotrebe kriptografski slabog MD5 algoritma za potpisivanje digitalnih sertifikata u SSL/TLS protokolima. Iako su kriptografi još 2005. godine (Wang i Yu) demonstrirali kolizije u MD5, ovaj algoritam se nastavio koristiti u sertifikacionim lancima i alatima za generisanje sertifikata, što je omogućilo da ranjivost opstane godinama bez zvanične zabrane. Eksploatacija je postala praktično izvodljiva tek nakon 2008. godine, kada su istraživači uspjeli kreirati sertifikate sa identičnim MD5 hash-om, čime se omogućava falsifikovanje i spoofing digitalnih potpisa. U mnogim verzijama OpenSSL-a MD5 je i dalje bio dozvoljen kao legitimna opcija za potpisivanje, bez upozorenja o njegovoj kriptografskoj slabosti, zbog čega su SSL/TLS implementacije nastavile da izdaju i prihvataju MD5-potpisane sertifikate sve do uvođenja modernijih sigurnosnih politika.

• **Primer Koda (ako je primenljivo):** Za ovu ranjivost ne postoji konkretan commit ili fajl koji sadrži grešku, ali suština problema leži u korišćenju slabih heš algoritama, poput MD5, bez provjere njihove bezbjednosti. U mnogim bibliotekama, kao što je OpenSSL, moguće je ručno odabrati MD5 prilikom potpisivanja sertifikata, što otvara prostor za napade bazirane na koliziji.

5. Preporuke za mitigaciju

• **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da. Iako sama ranjivost ne potiče iz greške u softverskom kodu, već iz korišćenja slabih algoritama prilikom izdavanja sertifikata, sertifikaciona tijela (CA) su od 2016. prestala izdavati nove sertifikate sa MD5 potpisima. Takođe, većina browsera i sistema od tada više ne priznaje takve sertifikate kao bezbjedne.

• **Mitigation Strategy:** Rješenje se sastoji u zamjeni svih SSL/TLS sertifikata koji koriste MD5 za potpisivanje, i njihovoj ponovnoj izradi korišćenjem sigurnog algoritma poput SHA-256 (ili jačeg). Postupak uključuje:

- Identifikaciju sertifikata sa slabim potpisom (npr. pomoću Nessus, Qualys SSL Labs, openssl x509 -text komande).
- Kontaktiranje nadležnog Certificate Authority (CA) i zahtjev za re-izdavanje sertifikata sa sigurnim hash algoritmom.
- Ponovno učitavanje sertifikata na serveru i restartovanje servisa (npr. Apache, Nginx, Tomcat).
- Preporučuje se i podešavanje servera da odbija klijente koji pokušaju pregovarati slabije algoritme, kroz TLS konfiguraciju (ssl_ciphers, ssl_protocols itd.).

• **Alternativni fix (ukoliko ne postoji vendorski):** Ukoliko trenutno nije moguće obnoviti sertifikate (npr. za starije interne servise), preporučuje se:

- Ograničiti pristup takvim servisima samo sa pouzdanih IP adresa (npr. kroz firewall),
- Onemogućiti pregovaranje slabih algoritama, posebno MD5, na nivou TLS konfiguracije (npr. SSLProtocol all -SSLv2 -SSLv3 i SSLCipherSuite HIGH:!MD5),
- Uvesti dodatne bezbjednosne slojeve, kao što su autentifikacija na aplikativnom nivou ili Web Application Firewall (WAF),
- Pratiti logove za potencijalne MITM pokušaje i nevalidne konekcije.