Vulnerability Assessment Report Template

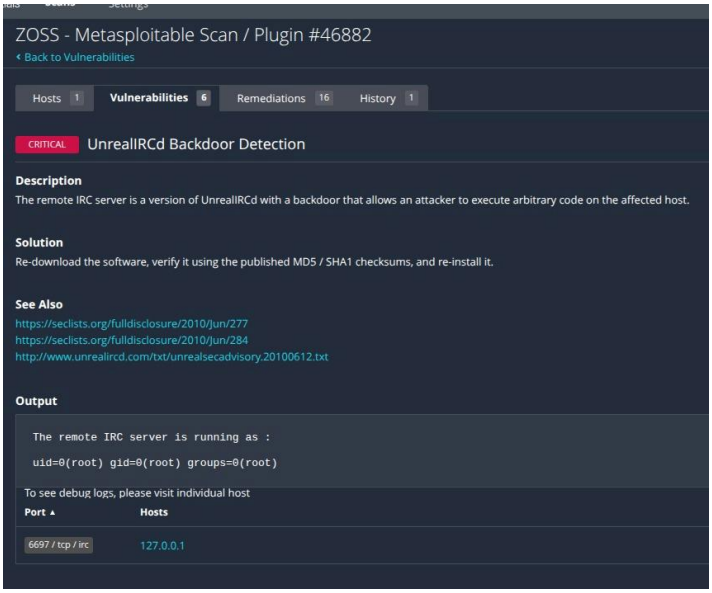
Ime i prezime: Dušica Trbović
Tim: ?
Datum: 21.12.2025.
Scan Tool: Nessus (10.11.1 (#21) LINUX)
Test okruženje: Metasploitable

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2010-2075

- **Opis:**
  CVE-2010-2075 predstavlja kritičnu bezbednosnu ranjivost u IRC serveru UnrealIRCd, koja je nastala kao posledica kompromitovane verzije softvera distribuirane sa ugrađenim backdoor-om. Ranjiva verzija UnrealIRCd omogućava udaljenom napadaču izvršavanje proizvoljnog koda na pogođenom sistemu bez potrebe za autentifikacijom. Backdoor se aktivira slanjem specijalno oblikovanih IRC komandi, nakon čega napadač dobija shell pristup sa privilegijama procesa koji pokreće servis. U test okruženju, ranjiv servis UnrealIRCd je detektovan na TCP portu 6667, koristeći IRC protokol. Nessus skener je identifikovao da se servis izvršava sa root privilegijama, što dodatno povećava ozbiljnost ove ranjivosti.



---

2. CVSS skor

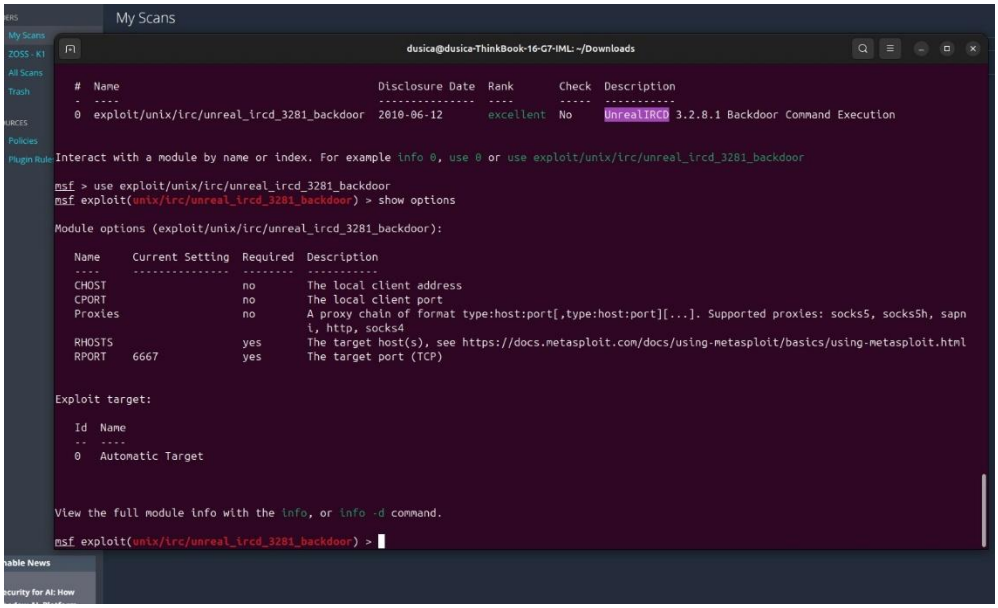
- **CVSS v2.0 Base Score:** 10.0 (Critical)
- **CVSS v2.0 Temporal Score:** 8.3
- **Vektor:** AV:N/AC:L/Au:N/C:C/I:C/A:C
- **Objašnjenje komponenti vektora:**
  - **AV:N** (Access Vector – Network):
    - Napad se može izvršiti preko mreže, bez fizičkog ili lokalnog pristupa sistemu.
  - **AC:L** (Access Complexity – Low):
    - Eksploatacija je jednostavna i ne zahteva posebne uslove ili kompleksne korake.
  - **Au:N** (Authentication – None):
    - Napadaču nije potrebna autentifikacija da bi iskoristio ranjivost.
  - **C:C** (Confidentiality Impact – Complete):
    - Potpuni gubitak poverljivosti – napadač može čitati sve podatke na sistemu.
  - **I:C** (Integrity Impact – Complete):
    - Potpuni gubitak integriteta – napadač može menjati podatke i izvršavati proizvoljan kod.
  - **A:C** (Availability Impact – Complete):
    - Potpuni gubitak dostupnosti – sistem može biti u potpunosti kompromitovan ili onesposobljen.
- **Opravdanje**
  Ova ranjivost ima maksimalan CVSS skor (10.0) jer omogućava udaljeno izvršavanje proizvoljnog koda bez ikakve autentifikacije, uz nisku kompleksnost napada.
  Backdoor je ugrađen direktno u kompromitovanu verziju softvera (UnrealIRCd 3.2.8.1), što znači da uspešna eksploatacija rezultuje potpunim preuzimanjem kontrole nad sistemom, uključujući kompromitovanje poverljivosti, integriteta i dostupnosti.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Da. Javno dostupan eksploit postoji i dostupan je kroz Metasploit Framework u okviru modula exploit/unix/irc/unreal_ircd_3281_backdoor.

- **Opis eksploita:**
  Eksploat koristi ugrađeni backdoor u verziji UnrealIRCd 3.2.8.1 koji omogućava napadaču da, bez autentifikacije, izvršava proizvoljne sistemske komande na udaljenom serveru putem IRC servisa na TCP portu 6667. Uspešna eksploatacija dovodi do potpunog kompromitovanja sistema.
- **Kod eksploita (ukoliko postoji):**
  Na slici je prikazan osnovni Metasploit modul koji koristi navedeni backdoor. Modul zahteva definisanje ciljnog hosta (RHOSTS) i ciljnog porta (RPORT), nakon čega omogućava izvršavanje proizvoljnih komandi na kompromitovanom sistemu.



---

4. Analiza uzroka (root cause)

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

  Ranjivost je uvedena u verziji UnrealIRCd 3.2.8.1, koja je tokom 2010. godine distribuirana sa ugrađenim zlonamernim backdoor kodom. Do problema nije došlo usled neadekvatne validacije ulaza ili logičke greške u aplikaciji, već kao posledica kompromitovanja zvanične distribucije softvera. Zlonamerni kod je dodat tokom procesa kompilacije ili pakovanja release verzije, čime je narušen integritet izvornog koda. Kao rezultat toga, napadač može slanjem posebno formirane IRC poruke da izvrši proizvoljne komande na pogođenom sistemu sa privilegijama procesa koji pokreće IRC server (u ovom slučaju root privilegije)..

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

  Izvorni kod backdoor mehanizma nije deo zvaničnog repozitorijuma, ali je njegova funkcionalnost dokumentovana kroz bezbednosne izveštaje i javno dostupne exploite. Postojanje ranjivosti potvrđeno je dostupnošću Metasploit modula

exploit/unix/irc/unreal_ircd_3281_backdoor, koji demonstrira izvršavanje proizvoljnih komandi na ciljanom sistemu.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):**
  Da.
  Zvanični vendor je uklonio backdoor i izdao bezbedne verzije UnrealIRCd-a nakon otkrivanja incidenta. Sve verzije novije od 3.2.8.1 ne sadrže ovu ranjivost, pod uslovom da su preuzete iz pouzdanog izvora i da je integritet paketa verifikovan.

- **Mitigation Strategy:**
  Preporučena strategija mitigacije je potpuna deinstalacija kompromitovane verzije UnrealIRCd 3.2.8.1 i instalacija bezbedne, novije verzije softvera preuzete isključivo sa zvaničnog sajta proizvođača. Pre instalacije, neophodno je izvršiti proveru integriteta paketa korišćenjem objavljenih MD5/SHA1 checksum vrednosti, kako bi se osiguralo da softver nije kompromitovan.
    - Dodatno, preporučuje se:
      - ograničavanje dostupnosti IRC servisa putem firewall pravila (dozvola samo pouzdanim IP adresama),
      - pokretanje servisa sa minimalnim privilegijama (ne kao root),
      - redovno ažuriranje sistema i praćenje bezbednosnih advisories proizvođača.

  U produkcionim okruženjima, proces ažuriranja može se automatizovati korišćenjem alata za upravljanje konfiguracijom i patch-ovanje sistema (npr. Ansible, Puppet, Chef).

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

  Ukoliko iz nekog razloga nije moguće odmah primeniti vendorski fix, alternativna mera je onemogućavanje ili uklanjanje UnrealIRCd servisa sa sistema, naročito ako IRC funkcionalnost nije kritična za rad sistema.

    - Kao privremeno rešenje, može se primeniti:

      - blokiranje IRC porta (6697/tcp) na firewall-u,
      - monitoring mrežnog saobraćaja radi detekcije sumnjivih IRC komandi,
      - izolacija kompromitovanog sistema iz mreže dok se ne izvrši bezbedna reinstalacija.