Probleme de securitate - Portalul IFEP

"Stefan Deleanu" <office@entryrise.com>
To: helpdesk@ifep.ro

February 28, 2023 at 1:46 PM

Buna ziua,

Va contactez pentru a raporta urmatoarele probleme de securitate informatica, pe care le-am identificat in timpul utilizarii platformei IFEP.

Am identificat urmatoarele probleme:

- **Bresa date cu caracter personal (Risc Ridicat):** API-ul accesibil AICI este public, si poate fi utilizat desi informatiile furnizate prin intermediul acestui API sunt informatii cu caracter personal. Spre exemplu, prin interogarea endpoint-ului "GetLawyersFull", un actor malicios poate obtine informatii referitoare la numele, prenumele, baroul unde sunt inregistrati, precum si CNP-ul persoanelor inscrise in tabloul furnizat de IFEP, care ar simplifica o potentiala uzurpare a calitatii de avocat de catre un astfel de actor.
- **Lista unui sistem de autentificare sigur (Risc Ridicat):** S-a apreciat ca utilizarea CNP-ului ca sistem unic de securizarea a platformei nu este o solutie ideala, fiind informatii care pot fi usor identificate sau deduse dupa un minim de analiza in informatiile disponibile publice. CNP-ul este format, in mare parte, din date asociate direct datei nasterii, genului, judetul nasterii, 3 numere care reprezinta seria nasterii (de la 001 la 999), precum si un cod de paritate calculat in baza celorlalte. Un atacator ar putea afla CNP-ul doar printr-un simplu bruteforce, cu 999 incercari, ulterior validand CNP-ul prin autentificarea reusita.
- **Potential risc de furt conturi (Risc Mediu):** In contextul in care un numar de telefon (neasociat contului) si CNP-ul profesionistilor sunt unicele date necesare pentru resetarea parolei, un atacator care cunoaste CNP-ul victimei ar putea sa se utilizeze de acesta, si un numar virtual, pentru a obtine acces in contul victimei.
- **Potential risc de deanonimizare a voturilor prin platforma (Risc Redus)**: In contextul problemelor sus mentionate, un atacator care dispune de CNP-ul persoanei (de pe care se poate obtine, in mod direct, codul CCBE), ar putea da bruteforce pe hash pentru a afla variabilele necunoscute (**CodSecuritate, Pozitii Votate).** In lipsa unui seed unic, atacul devine, de asemenea, exponential mai usor.

Recomandari de natura tehnica:

- Abordarea unei scheme de incredere "Zero Trust". Furnizarea minimului necesar de incredere utilizatorilor, pana la demonstrarea autorizatiei de accesare a datelor (spre exemplu, prin autentificarea intr-un cont cu privilegii).
- Modificarea schemei de autentificare cat aceasta sa includa informatii care nu pot fi deduse in baza informatiilor publice (Spre exemplu, prin utilizarea unui email si cod utilizator, si validarea manuala a cererilor de schimbare a parolei in baza unui document semnat cu semnatura electronica calificata).
- Restrictionarea accesului la API-uri interne, in contextul in care accesul nu este necesar pentru functionarea platformei.

Pentru orice detaliu de natura tehnica, sau orice alta intrebare, va stau la dispozitie pe email, sau telefonic.

Multumesc Mult,
Deleanu Stefan-Lucian

Stefan-Lucian Deleanu
Director / ENTRYRISE S.R.L

Website: www.entryrise.com
Email: office@entryrise.com
Phone: +40786833325