**CATRE:**
Consiliul Superior al Magistraturii
Directia Nationala de Securitate Cibernetica
Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu caracter personal

---

**Deleanu Stefan-Lucian**, identificat in baza CI CJ1001126, CNP 5021019330205, domiciliat in Judetul Cluj, Localitatea Cluj-Napoca, Strada Aurel Vlaicu, Nr 2, Bloc 5A, Sc I, Etaj 7, Apartament 28,

**Numar Telefon:** +40786833325
**Email contact:** office@incorpo.ro

---

În temeiul dispozițiilor Legii nr. 362/2018 coroborate cu prevederile O.G. nr. 27/2002 privind reglementarea activității de soluționare a petițiilor, formulez prezenta

# NOTIFICARE

Prin care vă aduc la cunoștință existența unor potențiale breșe de securitate în gestionarea domeniilor rejust.ro, csm1909.ro și emap.csm1909.ro aflate în proprietatea Consiliului Superior al Magistraturii (CSM), care ar permite actorilor rău intenționați să întreprindă următoarele acțiuni:

**Risc mediu: Crearea de subdomenii în scop personal (ex: blacklist.rejust.ro), cu aparență de legalitate,** datorită utilizării de către CSM a platformei "afraid.org" cu planul "shared-private" pentru găzduirea nameserverelor.

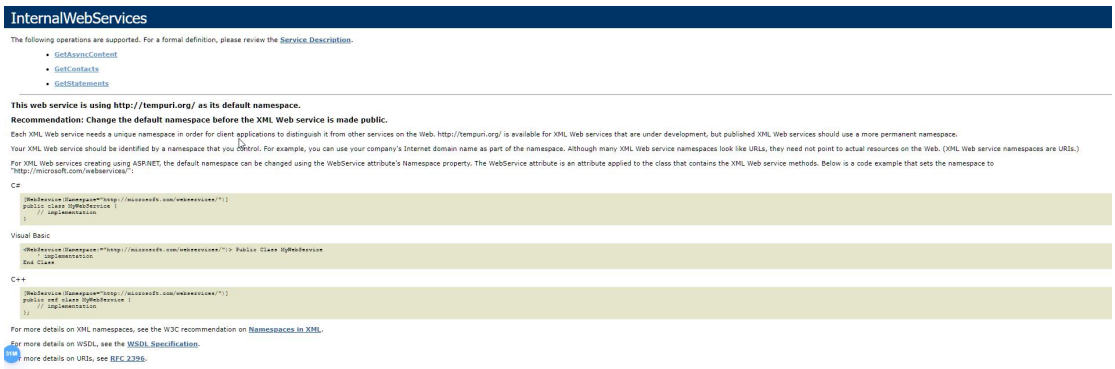
Condițiile de utilizare a acestui serviciu gratuit impun CSM să permită terților folosirea subdomeniilor în orice scop licit, singura posibilitate de retragere a acestui drept fiind catalogarea subdomeniilor drept denigratoare sau calomnioase. In plus, aleg sediul contractului ca fiind in California, in opinia noastra intregul acord fiind nul de drept.

Cu toate acestea, domeniile devin valabile instant, putând fi folosite de atacatori pentru autentificare prin înregistrări TXT, construirea de email-uri clandestine sau pagini web cu aparență de apartenență la CSM.

Spre exemplu, a se vedea domeniu http://stefan.rejust.ro, care va redictiona spre pagina de facebook a subsemnatului.

**2. Risc Redus: Extragerea tuturor utilizatorilor platformei csm1909.ro prin intermediul endpoint-urilor deschise ale https://www.csm1909.ro/WebServices.**

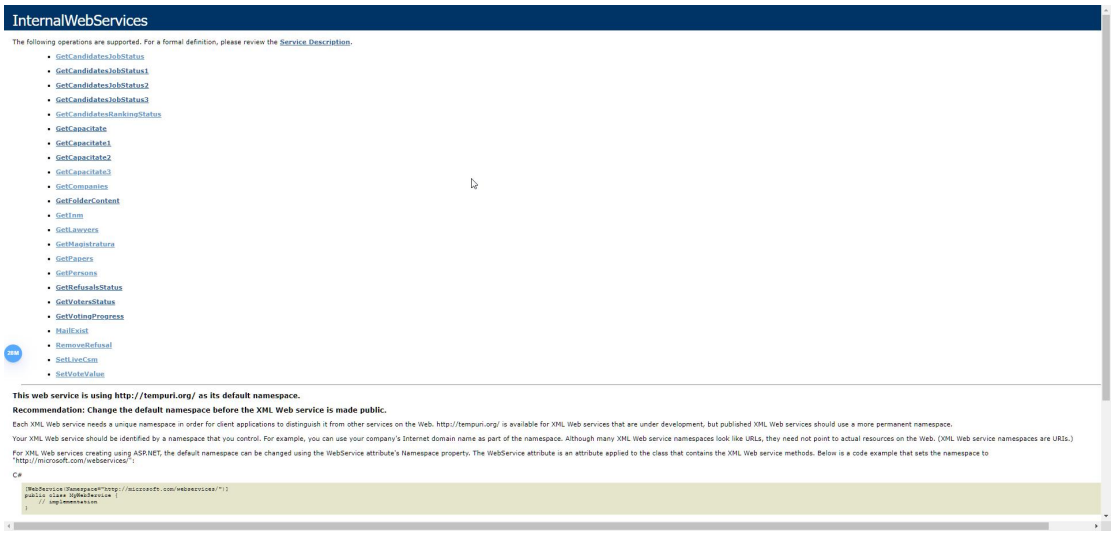
Obținerea contactelor membrilor CSM nu este necesară funcționării platformei și poate permite exfiltrarea datelor de identificare precum email-ul personal, numele și prenumele.




**3. Risc Redus: Obținerea adreselor de email personale în vederea unor atacuri de spear phishing, prin intermediul endpoint-ului de recuperare a parolei de pe https://emap.csm1909.ro.**

Coroborat cu vulnerabilitățile enunțate anterior, un atacator ar putea folosi un email autentificat pe domeniul mail.rejust.ro (ex: security@mail.rejust.ro) pentru a induce în eroare magistrații să își "reseteze" parola cu confirmarea celei anterioare din motive de securitate, obținând astfel parola originală în vederea escaladării privilegiilor pe platformă.

**4. Risc Ridicat: Potential lipsa autentificare endpoint-uri critice pe platforma emap** (https://emap.csm1909.ro/WebServices/InternalWebServices.asmx).




Platforma fiind analogul celei de pe www.ifep.ro, anterior notificată cu vulnerabilități care permiteau divulgarea CNP-urilor avocaților, există riscul ca emap.csm1909.ro, construită pe același structura, să prezinte probleme similare, având în vedere

cantitatea mare de endpoint-uri accesibile public. Printre endpoint-urile care pot implica riscuri în lipsa unei autentificări adecvate se numără:

**SetVoteValue:** fără autentificare, permite unui atacator care cunoaște ID-ul magistraților (probabil auto-incrementat, deci bruteforce-abil), ID-ul ședinței și buletinul de vot să falsifice voturile CSM pentru decizii critice în defavoarea magistraturii.

**MailExist:** permite validarea mail-urilor din sistemul emap.csm1909.ro care coroborate cu alte vulnerabilități pot fi folosite în atacuri de spear phishing. (clean baza de date scraped de mails pentru a nu intra in spam)

**RemoveRefusal:** probabil elimină veto-ul unui membru.

Lista completa de endpoint-uri este mai sus.

# PUNCT DE VEDERE

Având în vedere intensificarea atacurilor cibernetice, contextul geopolitic actual și importanța CSM în procesul democratic, consider necesară efectuarea unor audituri independente ale platformelor de către auditori de securitate cibernetică terți autorizați de DNSC (https://dnsc.ro/pagini/auditori-de-securitate-cibernetica), neimplicați în raportarea vulnerabilităților sau dezvoltarea platformelor.

Anterior, când am raportat vulnerabilități similare ale platformei ifep.ro (UNBR), societatea dezvoltatoare Intraconnect SRL nu a notificat avocații și probabil nici UNBR din motive economice (pentru a nu se decredibiliza). Chiar și în prezent, platforma are în continuare probleme de securitate din cauza lipsei de măsuri a UNBR ulterior notificării publice de către mine a vulnerabilităților, după 1 an de tăcere a UNBR.

În absența unor astfel de măsuri, riscurile de securitate rămân deschise.

**Cu stima,**

Deleanu Ștefan-Lucian