INSTITUTII:
Oficiul National al Registrului Comertului
Directoratul National de Securitate Cibernetica
Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal
Ministerul Justitiei

Subscrisa **ENTRYRISE S.R.L,** cu sediul social in B-dul. Bucovina, Bl. D 18, Sc. A, Et. 0, Ap. 2, Cod Poștal 725300, Gura Humorului, Jud. Suceava, CIF 43541700, EUID ROONRC.J33/46/2021

Reprezentata de

Deleanu Stefan-Lucian, in calitate de administrator cu puteri depline, 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

In temeiul dispozitiilor **OG 27/2002** corelat cu **OUG nr. 104/2021** si **LEGE nr. 190/2018,** va aducem la cunostinta urmatoarele:

Divulgarea coordonată și responsabilă a vulnerabilităților

Cu privire la identificarea unor vulnerabilitati a implementarii “MyPortal”, parte a proiectului Sistem Electronic Integrat al ONRC consolidat și interoperabil destinat asigurării serviciilor de e-Guvernare centrate pe evenimente de viață (ONRC V2.0):

Risc Ridicat:

S-a identificat o vulnerabilitate severă pe platforma ONRC care permite oricărei persoane să obțină informații cu caracter personal, cum ar fi CNP-ul și adresa de domiciliu, ale persoanelor care efectuează plăți prin intermediul notelor de calcul.

Probleme:

1. Lipsa unui sistem de autentificare și control al accesului la notele de calcul. Oricine poate accesa notele de calcul ale altei persoane.

2. Existența unei funcții de abonare la notele de calcul ale terților, facilitând obținerea datelor specifice ale unei persoane țintă.

3. Lipsa unui sistem de validare efectiv al cererilor depuse si solutionate automat care genereaza riscuri de expunere pentru ONRC.

4. Expunere inutila a unor date care pot fi sensibile, inclusiv date cu caacter personal, datorita funrnizarii tuturor informatilor prin utilizarea functiei de “INFORMARE - STADIU DOSAR”

5. Expunerea tuturor CNP-urilor persoanelor declarate insolvente (BPI) datorita edivulgarii de catre endpoint a acestuia. (corelat cu nume-prenume)

6. Lipsa verificarii statusului de plata la furnizare raport beneficari (obtinere fara plata informatii).

Vulnerabilitatea 1:

Lipsa unui sistem de autentificare și control al accesului la notele de calcul. Oricine poate accesa notele de calcul ale altei persoane.

Pasi de reproducere:

1. Crearea unui cont pe platforma ONRC.

2. Accesarea unui URL de forma "https://myportal.onrc.ro/calculation-note-summary/NC2024XXXXXXXX", unde XXXXXXXX reprezintă un număr serial.

   Exemplu: https://myportal.onrc.ro/calculation-note-summary/NC202400001620

3. Descărcarea notei de calcul care conține date personale sensibile ale solicitantului, cum ar fi CNP-ul și adresa.

Impactul potențial:

În momentul raportării, cel puțin 1630 de cereri expun CNP-ul solicitanților în mod direct pe platformă, precum si domiciliul lor. Deși în cazul persoanelor juridice datele pot fi mai puțin sensibile, pentru persoanele fizice această breșă reprezintă un risc major de fraudă și furt de identitate.

Recomandări:

1. Implementarea de urgență a unui sistem de autentificare și control al accesului pentru a restricționa vizibilitatea notelor de calcul doar pentru utilizatorii autorizați.

2. Eliminarea funcției de abonare la notele de calcul ale terților.

3. Re-auditarea platformei pentru a identifica și remedia orice alte vulnerabilități potențiale.

4. Notificarea persoanelor afectate cu privire la această breșă de securitate și oferirea de îndrumări pentru a-și proteja identitatea.

Vulnerabilitatea 2:

Obtinerea tuturor CNP-urilor persoanelor fizice in stare de insolventa precum si informatiilor din BPI, cu un program si documente semnate electronic complet nerelevante situatiei si care nu permit identificarea si sanctionarea faptuitorului.

Pasi de reproducere:

1. Crearea unui cont pe platforma ONRC.
2. Accesarea https://myportal.onrc.ro/bpi-published-persons/pf si introducerea unei vocale (eg"a")
3. Se vor obtine toate datele (nume, prenume, CNP, date sistem intern) despre persoanele respective, in raspunsul JSON dat de server.
4. CNP-ul nu este necesar a fi furnizat pentru 235 de persoane.
5. Utilizarea vulnerabilitatii cumulata cu vulnerabilitatea lipsei de plati poate fi folosita pentru exfiltrarea de informatii suplimentare, precum judetul si localitatea de domiciliu.

Impactul potențial:

În momentul raportării, 235 de persoane fizice insolvente au fost identificate cu CNP-ul public.

Recomandări:

1. Limitarea din backend a furnizarii de informatii care nu sunt necesare pentru randarea in UI, si implementarea unui sistem need-to-know care sa se extinda si sistemului informatic si permissioning-ului din platforma.
2. Re-auditarea platformei pentru a identifica și remedia orice alte vulnerabilități potențiale.
3. Notificarea persoanelor afectate cu privire la această breșă de securitate și oferirea de îndrumări pentru a-și proteja identitatea.

Vulnerabilitatea 3:

Expunere inutila a unor date care pot fi sensibile, inclusiv date cu caacter personal, datorita funrnizarii tuturor informatilor prin utilizarea functiei de "INFORMARE - STADIU DOSAR"

Pasi de reproducere:

1. Crearea unui cont pe platforma ONRC.

2. Accesarea https://myportal.onrc.ro/dossier-status si introducerea CUI-ului societatii de unde se vor obtine informatii.

3. Verificarea datelor obtinute de browser, spre exemplu din tab-ul networking din inspect element, sau alternativ, cu un program precum Fiddler

Impactul potențial:

În momentul raportării, toate societatile inregistrate in Romania sunt vulnerabile exfiltrarii de informatii prin acest mod. Datorita lipsei unor limitari efective de request-uri pe secunda, se pot efiltra toate datele intr-o seara.

Datele includ:

- Datele de contact communicate prin cereri catre ONRC
- Informatii despre societati sau persoane fizice autorizate, de la activitatile societatii, numarul de parti sociale, registrator in speta, durata societatii, status insolventa, etc
- numar telefon contact, numar fax, posibil email declarat ONRC,
- toate punctele de lucru declarate ONRC,
- toate informatiile cu privire la chiria spatiului, intrarea in vigoare si expiraarea expirarea (durata) acestora, furnizor chirie (inclusiv persoana fizica),
- detalii infrastructura backoffice, detalii documente depuse de persoane, detalii registratori implicati (clona BERC), detalii acte si gradul lor de clasificare (?)

Recomandări:

1. Limitarea din backend a furnizarii de informatii care nu sunt necesare pentru randarea in UI, si implementarea unui sistem need-to-know care sa se extinda si sistemului informatic si permissioning-ului din platforma.

2. Re-auditarea platformei pentru a identifica și remedia orice alte vulnerabilități potențiale.

3. Notificarea persoanelor afectate cu privire la această breșă de securitate și oferirea de îndrumări pentru a-și proteja identitatea

Vulnerabilitatea 4:

Obtinerea de documente in format electronic prin utilizarea unui portofel gol, sistemul ne-avand absolut nici o validare cu privire la solvabilitatea portofelului utilizatorului.

Pasi de reproducere:

1. Crearea unui cont pe platforma ONRC.

2. Accesarea si completarea oricarei cereri cu furnizare instant (eg: buletin proceduri insolventa, certificate constatoare, certificate beneficiari reali, etc).

3. Ignorarea notei de calcul primite si verificarea dosarului in https://myportal.onrc.ro/my-requests

Impactul potențial:

În momentul raportării, toate societatile inregistrate in Romania sunt vulnerabile exfiltrarii de informatii prin acest mod. Datorita lipsei unor limitari efective de request-uri pe secunda, se pot efiltra toate datele intr-o seara.

Datele includ:

- Datele de contact communicate prin cereri catre ONRC
- Informatii despre societati sau persoane fizice autorizate, de la activitatile societatii, numarul de parti sociale, registrator in speta, durata societatii, status insolventa, etc
- numar telefon contact, numar fax, posibil email declarat ONRC,
- toate punctele de lucru declarate ONRC,
- toate informatiile cu privire la chiria spatiului, intrarea in vigoare si expiraarea expirarea (durata) acestora, furnizor chirie (inclusiv persoana fizica),
- detalii infrastructura backoffice, detalii documente depuse de persoane, detalii registratori implicati (clona BERC), detalii acte si gradul lor de clasificare (?)

Recomandări:

1. Limitarea din backend a furnizarii de informatii care nu sunt necesare pentru randarea in UI, si implementarea unui sistem need-to-know care sa se extinda si sistemului informatic si permissioning-ului din platforma.

2. Re-auditarea platformei pentru a identifica și remedia orice alte vulnerabilități potențiale.

3. Notificarea persoanelor afectate cu privire la această breșă de securitate și oferirea de îndrumări pentru a-și proteja identitatea

Risc Mediu:

Formularile din termeni si conditii, prin care ONRC isi limiteaza raspunderea civila delictuala prin a informa utilizatorii de riscurile ca datele lor sa fie accesibile public, intrucat securitatea datelor lor este oferita pe sistem “best effort”, in primul rand nu sunt probabil legale, in al doilea rand, denota ca ONRC a avut raportate mai multe vulnerabilitati prin audit-urile interne efectuate.

Utilizatorul ia la cunoștință că Serviciile sunt disponibile prin Internet și deși ONRC va face tot posibilul pentru a menține securitatea informațiilor, nu poate garanta că informația pe care Utilizatorul o primește sau o trimite folosind Serviciile va fi permanent în siguranță. **(extras din cod sursa)**

Nu stim daca a fost prudenta lansarea platformei, in contextul in care este cert ca versiunea este una de staging. O solutie mai eficienta ar fi fost implementarea progresiva, sau in cazul in care ea implica costuri suplimentare semnificative, o testare mai corecta a aplicatiei, dpdv. al prezentei de vulnerabilitati.

Desi utilizarea de UUID-uri face dificila obtinerea datelor despre o cerere a unui tert, tendinta utilizatorilor de a face screenshot-uri, a transmite URL-uri la terti poate genera astfel situatii in care datele lor devin accesibile public. **Bazarea pe securitate prin obscuritate nu este o strategie eficienta unei entitati publice esentiale.**

Risc Scazut:

Pași pentru a reproduce vulnerabilitatea 4:

Pasi de reproducere:

1. Crearea unui cont pe platforma ONRC.

2. Accesarea si completarea cererii de rezervare denumire pana la pasul generarii documentului. Se va genera documentul, descarca, si salva cererea.

3. In paralel, se va lua o pagina goala de PDF, si se va semna cu o semnatura electronica calificata. Se va da rename la acel PDF gol cu numele cererii generate de platforma. Se va da upload, iar platforma o va accepta dat fiind ca are acelasi nume de fisier.

4. Sistemul va aproba in mod automat acest document gol desi el nu reprezinta o cerere efectiva.

Impactul potențial:

În momentul raportării, cel puțin 1630 de cereri expun CNP-ul solicitanților în mod direct pe platformă. Deși în cazul persoanelor juridice datele pot fi mai puțin sensibile, pentru persoanele fizice această breșă reprezintă un risc major de fraudă și furt de identitate.

Recomandări:

1. Implementarea de urgență a unui sistem de autentificare și control al accesului pentru a restricționa vizibilitatea notelor de calcul doar pentru utilizatorii autorizați.

2. Eliminarea funcției de abonare la notele de calcul ale terților.

3. Re-auditarea platformei pentru a identifica și remedia orice alte vulnerabilități potențiale.

4. Notificarea persoanelor afectate cu privire la această breșă de securitate și oferirea de îndrumări pentru a-și proteja identitatea.

Concluzie

Considerăm că severitatea și impactul potențial al vulnerabilităților identificate sunt extrem de ridicate. Există un risc semnificativ ca aceste probleme de securitate să fie exploatate de actori rău-intenționați, ceea ce ar duce la expunerea datelor a milioane de cetățeni și companii din România.

Deși numărul persoanelor afectate direct (cum ar fi persoanele fizice insolvente și utilizatorii MyPortal) poate părea relativ mic, sub 5000, nu trebuie să ignorăm potențialul impact mai larg:

Datele expuse, cum ar fi CNP-urile, adresele și informațiile financiare, pot fi folosite de infractori pentru a comite fraude de identitate, spearphishing targetat și alte infracțiuni cibernetice. Aceste atacuri pot afecta un număr mult mai mare de cetățeni și companii.

Scurgerile de date de la ONRC pot submina încrederea publică în instituțiile statului și în siguranța serviciilor guvernamentale digitale. Acest lucru poate descuraja adoptarea și utilizarea platformelor de e-guvernare.

Informațiile sensibile deținute de ONRC, chiar dacă sunt parțial publice, nu ar trebui să fie accesibile în masă fără restricții. Agregarea și corelarea ușoară a acestor date le crește valoarea pentru actorii rău intenționați și riscul de abuz.

Ca instituție publică esențială, ONRC are obligația legală și morală de a proteja în mod adecvat datele pe care le colectează și le procesează. Eșecul de a face acest lucru poate atrage sancțiuni, daune reputaționale și pierderea încrederii publice.

Prin urmare, vă îndemnăm să tratați aceste vulnerabilități cu cea mai mare seriozitate și urgență.

Solicităm ONRC să ia măsuri imediate pentru a aborda aceste vulnerabilități critice, inclusiv:

1. **Blocarea temporară a accesului la platforma MyPortal până la remedierea problemelor tehnice**

2. Implementarea unui sistem robust de autentificare și control al accesului
3. Limitarea cantității de date transmise către utilizatori pe bază de necesitate
4. Efectuarea unui audit de securitate extins și aprofundat al întregii platforme
5. Notificarea persoanelor și entităților afectate de potențialele breșe de date

De asemenea, **solicităm DNSC să supravegheze îndeaproape procesul de remediere și să se asigure că ONRC ia toate măsurile necesare pentru a proteja datele cetățenilor**.

Mai mult, intrucat Romania sufera de o sub-raportare a incidentelor de incalcare a securitatii datelor cu caracter personal, iar finalmente, victimele trebuie sa cunoasca si sa aiba dreptul sa decida ce masuri sa ia pentru a isi proteja informatiile cu caracter personal, **am notificat ANSPDCP, in speranta sanctionarii unei potentiale tentative de ne-raportare a incidentului, practrica fiind frecventa si in randul institutiilor publice.**

Datorita importantei gestionarii eficiente a proiectelor de gen a institutiilor subordonate Ministerului Justitiei, ministerul a fost in mod direct adaugat in lista de destinatari, pentru ca ulterior incidentului, sa poata analiza reactia si sa ia masuri pe viitor pentru a preveni astfel de incidente din a se mai repeta pe viitor.

Vă rugăm să ne comunicați în cel mai scurt timp planul de acțiune și calendarul pentru abordarea acestor probleme critice de securitate. Ne rezervăm dreptul de a informa publicul cu privire la aceste vulnerabilități dacă nu sunt soluționate prompt și complet, pentru a permite cetățenilor și companiilor să-și ia propriile măsuri de precauție.

Cu deosebită considerație,

ENTRYRISE S.R.L

prin Deleanu Stefan-Lucian

[SEMNAT ELECTRONIC]