Deleanu Ștefan-Lucian, identificat prin C.I. seria CJ nr. 1001126, având CNP 5021019330205, domiciliat in județul Cluj, Localitatea Cluj-Napoca, Strada Aurel Vlaicu, Nr 2, Bloc 5A, Sc I, Etaj 7, Apartament 28, in calitate de petent,

În temeiul ORDONANȚEI DE URGENȚĂ nr. 104 din 22 septembrie 2021, va aducem la cunostinta o serie mai mare de vulnerabiltiati descoperite de-a randul anilor, care au fost raportate institutiilor vulnerabile, sau sunt recente, si care nu s-au soldat cu solutionarea vulnerabilitatilor.

Recent, ni s-a adus la cunostinta existenta DNSC, si o aparenta capabilitate operationala care sa permita sau cel putin sa incurajeze solutionarea reala a problemelor, pe termen lung.

Lista include vulnerabilitati vechi, inca nerezolvate la data notificarii DNSC. Urmam de acum sa notificam si DNSC, in prealabil, spre a se asigura ca institutiile nu se eschiveaza de la rezolvarea problemelor.

In fundamentarea notificarii, am abordat tema cu un grad de ironie si frustrare, atribuit oboselii (redactare la ora 1:48 dimineata), si unei frustrari ca dupa demersurile luate de a notifica, unii operatori nu au luat de loc in seama mentiunile, desi unele sunt din domenii extrem de sensibile.

Faptul ca exista riscul ca actori stat sa “publice legi” pe RAMO si nu se ia in serios e cat se poate de grav.

Vom incerca saptamanile viitoare sa identificam toate mail-urile de pe care s-au notificat institutiile de existenta breselor, pentru a include si alte notificari, dintre cele pe care nu le retin.

Sumar vulnerabilitati:

1. Monitorul Oficial - SQL Injection + Directory Traversal (and listing) + endpoint-uri publice + backup-uri in foldere publice, neparolate.
2. Instante din Romania (82% din toate instantele) cu soft Arad - Autentificare slaba + lipsa robots.txt + link-uri fara autentificare acces date dosar (indexare pe google solutii cu date sensibile)
3. Curtea de Apel Cluj - Directory traversal + backup-uri in foldere publice, neparolate + certificat VPN accesibil publice.
4. Biblioteca Nationala Romana - Upload nesanitizat fisiere (inclusiv fisiere executabile .php)

Timp propus pentru remediere:

1. Monitorul oficial (Expert-Monitor) - 6 luni: Patch SQL injection in maxim 2 saptamani, solutie permanenta in 6 luni. Deja nu au facut nimic din 17 Octombrie 2022.

2. Instante din Romania - 3 luni: Patch robots.txt in maxim 1 saptamana + solicitare google search console de de-indexare link-uri deja crawluite.

Implementare sistem de ratelimiting pe IP si pe cont in 1 luna (ambele, care apare primul)

Implementare sistem de autentificare in 2 pasi si rezolvare problema upload - **3 luni**

3. Curtea de Apel Cluj - 2 Saptamani: Eliminarea fisierelor accesibile si validarea ca nu pot fi accesibile in 1 saptamana.

Rezolvarea directory listing in 2 saptamani.

4. Biblioteca Nationala - Platforma Web - 1 Saptamana: Dar nu credem ca au competentele sau disponibilitatea / dorinta sa rezolve (au refuzat sa rezolve in mod anterior) si cand i-am contactat telefonic sa le invederam riscurile, echipa IT nu a inteles explicatiile extrem de simple.

Timp propus pentru publicare:

1 luna dupa confirmarea solutionarii vulnerabilitatilor, si auditarea pentru prevenirea tentativelor de a descoperi alte vulnerabilitati similare.

Modalitatea în care doriti să publicati: Comunicat de presa

Doresc să fiu contactat de către Deținător: Da

Sunt de acord să fiu intervievat/menționat pe pagina CERT-RO, dacă mi se solicită acest lucru: Da

Declarații (trebuie să se regăsească la finalul raportării transmise):

· Declar pe proprie răspundere că datele furnizate sunt corecte, complete și corespund adevărului;

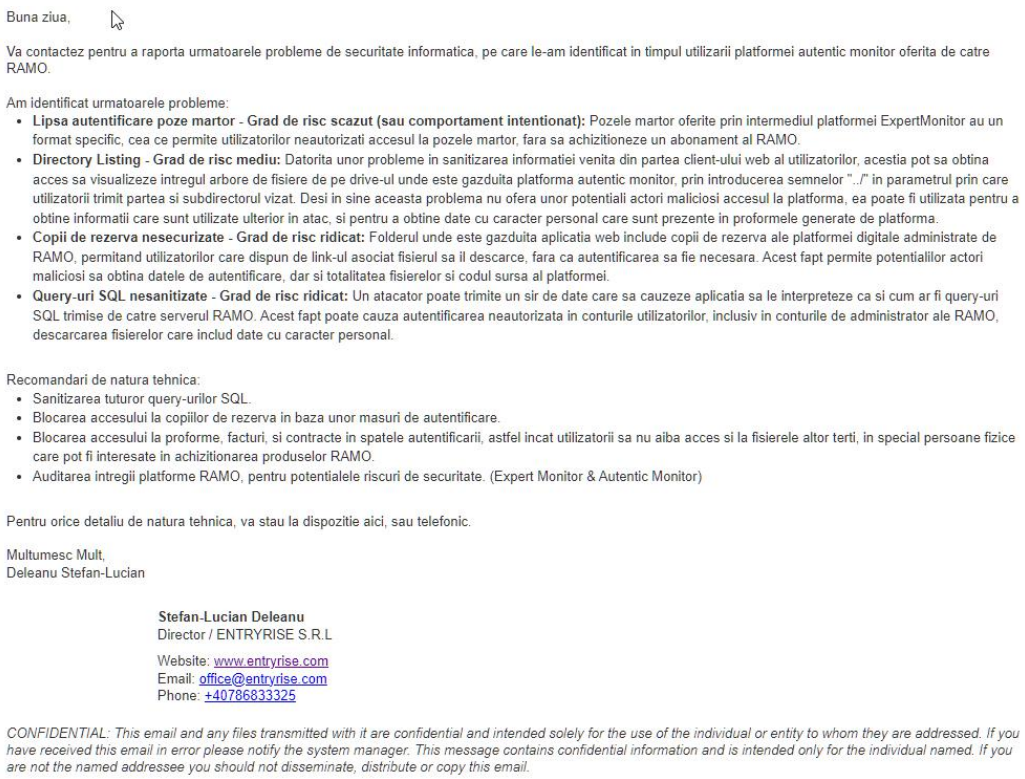
· Declar că am luat la cunoștință de Ghidul de raportare, Termenii și condițiile și Procedura de notificare prin CERT-RO și sunt de acord cu acestea.

Abonare:

· Doresc ca adresa mea de email să fie inclusă în lista de anunțuri generale referitoare la programul CVD al CERT-RO: NU

APLICATIE “EXPERT-MONITOR” - MONITORUL OFICIAL

O vulnerabilitate identificata, si cel mai probabil ne-rezolvata in totalitate, este vulnerabilitatea de la Monitorul Oficial, raportata pe Octombrie 17, 2022.



Buna ziua,

Va contactez pentru a raporta urmatoarele probleme de securitate informatica, pe care le-am identificat in timpul utilizarii platformei autentic monitor oferita de catre RAMO.

Am identificat urmatoarele probleme:

- **Lipsa autentificare poze martor - Grad de risc scazut (sau comportament intentionat):** Pozele martor oferite prin intermediul platformei ExpertMonitor au un format specific, cea ce permite utilizatorilor neautorizati accesul la pozele martor, fara sa achizitioneze un abonament al RAMO.
- **Directory Listing - Grad de risc mediu:** Datorita unor probleme in sanitizarea informatiei venita din partea client-ului web al utilizatorilor, acestia pot sa obtina acces sa visualizeze intregul arbore de fisiere de pe drive-ul unde este gazduita platforma autentic monitor, prin introducerea semnelor "../" in parametrul prin care utilizatorii trimit partea si subdirectorul vizat. Desi in sine aceasta problema nu ofera unor potentiali actori maliciosi accesul la platforma, ea poate fi utilizata pentru a obtine informatii care sunt utilizate ulterior in atac, si pentru a obtine date cu caracter personal care sunt prezente in proformele generate de platforma.
- **Copii de rezerva nesecurizate - Grad de risc ridicat:** Folderul unde este gazduita aplicatia web include copii de rezerva ale platformei digitale administrate de RAMO, permitand utilizatorilor care dispun de link-ul asociat fisierul sa il descarce, fara ca autentificarea sa fie necesara. Acest fapt permite potentialilor actori maliciosi sa obtina datele de autentificare, dar si totalitatea fisierelor si codul sursa al platformei.
- **Query-uri SQL nesanitizate - Grad de risc ridicat:** Un atacator poate trimite un sir de date care sa cauzeze aplicatia sa le interpreteze ca si cum ar fi query-uri SQL trimise de catre serverul RAMO. Acest fapt poate cauza autentificarea neautorizata in conturile utilizatorilor, inclusiv in conturile de administrator ale RAMO, descarcarea fisierelor care includ date cu caracter personal.

Recomandari de natura tehnica:

- Sanitizarea tuturor query-urilor SQL.
- Blocarea accesului la copiilor de rezerva in baza unor masuri de autentificare.
- Blocarea accesului la proforme, facturi, si contracte in spatele autentificarii, astfel incat utilizatorii sa nu aiba acces si la fisierele altor terti, in special persoane fizice care pot fi interesate in achizitionarea produselor RAMO.
- Auditarea intregii platforme RAMO, pentru potentialele riscuri de securitate. (Expert Monitor & Autentic Monitor)

Pentru orice detaliu de natura tehnica, va stau la dispozitie aici, 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

CONFIDENTIAL: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this email.

Nu am primit nici un raspuns. Telefonic (cand am contactat noi RAMO) ni s-a spus ca au inteles ca noi dorim sa ne facem marketing si ne-au invitat in Bucuresti pentru o discutie. Am refuzat, mentionand ca suntem dispusi sa ajutam, in limitele timpului, pro bono, insa nu pentru dezvoltarea altei platforme, pe banii statului.

Ne-au spus ca au notificat pe cine trebuie dar nu pot spune numele la telefon (Probabil SRI sau STS), dar aparent nu s-au luat masuri.

Nu credem ca s-a rezolvat problema la aplicatia “Expert-monitor.ro” sub nici o forma, desi gravitatea este enorma.

Spre exemplu, si acum este directory listing la toate proformele si facturile, probabil si SQL Injection si de acolo si riscul ca cineva sa gaseasca cum sa publice “o lege”:

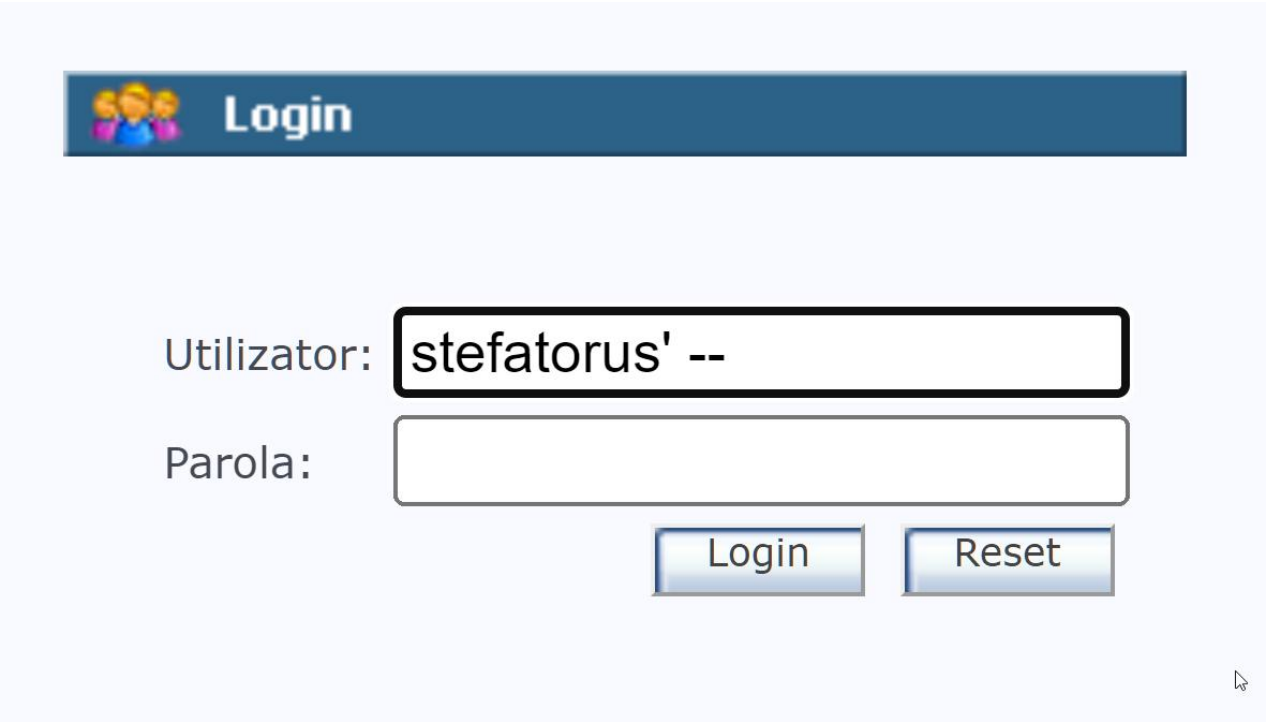
https://www.expert-monitor.ro/LexMonitorMBM/comercial/facturi/
https://www.expert-monitor.ro/LexMonitorMBM/comercial/proforme/

Am testat endpoint-ul de login, anterior vulnerabil:

“https://www.expert-monitor.ro/LexMonitorMBM/comercial/clientextern/login.php” care inca sufera de vulnerabilitate de SQL injection

Mijloc de reproducere:

1. In campul de utilizator se introduce:



2. Se apasa login.

Riscul este insa exponentiat cand tinem cont ca prin aceiasi platforma, si tot printr-un user, se autentifica si adminii platformei RAMO.

Probabil, cu alt cod SQL, se poate selecta primul user dupa ID, care probabil e admin, sau iterativ, a se itera prin toti userii, pana se ajunge la un cont admin.

Cum se permite cod arbitrar se poate sterge baza de date sau din contra, pe un endpoint care afiseaza ceva, exporta baza de date. Sau introduce date arbitrar, pe alte endpoint-uri.

In contextul in care ar exista SQL injection, ne este teama ca o astfel de bresa, cumulata cu celelalte descoperite anterior (neverificate acum pentru ca nu am reinnoit abonamentul RAMO), **se poate obtine acces la intreaga platforma si publica sau modifica legi.**

APLICATIE “TRIBUNALUL ARAD” – DOCUMENTE INSTANTA

Aplicatia dezvoltata de tribunalul arad, in versiunea 1.7.2, are erori de design care genereaza riscul indexarii a unor documente care includ date sensibile, cu caracter personal sau secret (de serviciu), in spatiul public.

Suplimentar, consideram ca mijlocul de autentificare, prin intermediul email-ului, printr-un endpoint cu ratelimit de reincercare la autentificare pe cookie (se poate face bruteforce cel mai probabil), cu o parola de 6 caractere numerice (1 milion combinatii), este unul care genereaza riscuri de a permite unor actori maliciosi sa obtina date sensibile.

In al treilea rand, un risc semnificativ este cauzat de faptul ca anumite documente, fie in mod manual, fie in mod automat, sunt atasate cererii:

HOSTNAME/uploads/<NR INSTANTA PUBLIC>/<NR DOSAR FLATTENED>/<NR PREDICTIBIL>_signed.pdf

Riscul prezicerii fisierelor creste cu atat mai mult prin faptul ca s-a omis introducerea unui fisier robots.txt, care sa previna indexarea si crawling-ul de catre robotii motoarelor de cautare:

Spre exemplu:

https://www.google.com/search?q=site%3Adoc.tmb.ro%2Fuploads

In total, 33 de rezultate de hotarari / dovezi / citari ale instantelor, care nu ar trebui sa fie publice, si care includ CNP-ul persoanelor respective.

In toata tara, par a fi **aproximativ 50-60 de solutii / documente procedurale indexate de Google**.

filetype:pdf site:doc.ca-iasi.ro OR site:doc.cab1864.eu OR site:doc.cagl.ro OR site:doc.caploiesti.ro OR site:doc.cma.ro OR site:doc.curteadeapelalbaiulia.ro OR site:doc.curteadeapelcraiova.eu OR site:doc.curteadeapelsuceava.ro OR site:doc.curteapelconstanta.eu OR site:doc.curteapeltimisoara.ro OR site:doc.iccj.ro OR site:doc.tmb.ro OR site:doc.tribunalularad.ro OR site:doc.tribunalulbotosani.ro OR site:doc.caploiesti.ro OR site:doc.curteadeapelbrasov.ro OR site:doc.curteadeapelmures.ro OR site:doc.curteadeapeloradea.ro

In timp ce probabil sunt vinovati ca au postat link-ul pe un format care a permis ulterior descoperirea si indexarea link-ului, acest fapt nu scuza lipsa unui fisier robots, care de altfel, nu este dificil de implementat pe tot folderul mentionat supra.

Afectate sunt astfel urmatoarele instante, cu o probabilitate ridicata sa fie mai multe (S-au identificat cu un query pe google):

https://www.google.com/search?q=%22Speciali%C8%99tii+IT+ai+Tribunalului+ARAD%22

In total, urmatoarele instalatii separate sunt afectate:

https://doc.ca-iasi.ro/
https://doc.cab1864.eu/
https://doc.cagl.ro/
https://doc.caploiesti.ro/
https://doc.cma.ro/
https://doc.curteadeapelalbaiulia.ro/
https://doc.curteadeapelcraiova.eu/
https://doc.curteadeapelsuceava.ro/
https://doc.curteapelconstanta.eu
https://doc.curteapeltimisoara.ro/
https://doc.iccj.ro/
https://doc.tmb.ro/
https://doc.tribunalularad.ro/
https://doc.tribunalulbotosani.ro/
https://doc.caploiesti.ro/
https://doc.curteadeapelbrasov.ro/
https://doc.curteadeapelmures.ro/
https://doc.curteadeapeloradea.ro/

Astfel, aproximativ 196/238 instante folosesc sisteme care sunt vulnerabile, fiind posibil sa fi omis cateva.

Tribunalul Vrancea, Tribunalul Vaslui, Tribunalul Tulcea, Tribunalul Timiș, Tribunalul Teleorman, Tribunalul Suceava, Tribunalul Specializat Mureș, Tribunalul Sibiu, Tribunalul Satu Mare, Tribunalul Prahova, Tribunalul Olt, Tribunalul Mureș, Tribunalul Minori si Familie Brasov, Tribunalul Militar Timisoara, Tribunalul Militar Iasi, Tribunalul Militar Cluj, Tribunalul Militar Bucuresti, Tribunalul Mehedinti, Tribunalul Ilfov, Tribunalul Iasi, Tribunalul Ialomita, Tribunalul Hunedoara, Tribunalul Harghita, Tribunalul Gorj, Tribunalul Giurgiu, Tribunalul Galați, Tribunalul Dolj, Tribunalul Dambovita, Tribunalul Covasna, Tribunalul Constanța, Tribunalul Caraș-Severin, Tribunalul Calarasi, Tribunalul Buzau, Tribunalul București, Tribunalul Bucuresti Asigurari, Tribunalul Brăila, Tribunalul Brasov, Tribunalul Bihor, Tribunalul BOTOȘANI, Tribunalul Alba, Tribunalul ARAD, Judecătoria Însurăței, Judecătoria Vatra Dornei, Judecătoria Tîrgu Bujor, Judecătoria Târnăveni, Judecătoria Târgu-Mureș, Judecătoria Tulcea, Judecătoria Toplița, Judecătoria Timișoara, Judecătoria Tecuci, Judecătoria SĂVENI, Judecătoria Sânicolau Mare, Judecătoria Suceava, Judecătoria Sighișoara, Judecătoria Sectorului 6, Judecătoria Sectorului 5, Judecătoria Sectorului 4, Judecătoria Sectorului 3, Judecătoria Sectorului 2, Judecătoria Sectorului 1, Judecătoria Salonta, Judecătoria Rădăuți, Judecătoria Reșița, Judecătoria Reghin, Judecătoria Panciu, Judecătoria Oravița, Judecătoria Oradea, Judecătoria Odorheiu Secuiesc, Judecătoria Măcin, Judecătoria Moldova-Nouă, Judecătoria Medgidia, Judecătoria Marghita, Judecătoria Mangalia, Judecătoria Lugoj, Judecătoria Luduș, Judecătoria Liești, Judecătoria LIPOVA, Judecătoria INEU, Judecătoria Hârșova, Judecătoria Gura Humorului, Judecătoria Gheorgheni, Judecătoria GURAHONȚ, Judecătoria Făurei, Judecătoria Fălticeni, Judecătoria Făget, Judecătoria Focșani, Judecătoria Deta, Judecătoria DOROHOI, Judecătoria DARABANI, Judecătoria Câmpulung Moldovenesc, Judecătoria Constanța, Judecătoria Caransebeș, Judecătoria CHIȘINEU-CRIȘ, Judecătoria Brăila, Judecătoria Beiuș, Judecătoria Babadag, Judecătoria BOTOȘANI, Judecătoria Aleșd, Judecătoria Adjud, Judecătoria ARAD, Judecatoria Zimnicea, Judecatoria Zarnesti, Judecatoria Videle, Judecatoria Vaslui, Judecatoria Vanju Mare, Judecatoria Valenii de Munte, Judecatoria Urziceni, Judecatoria Turnu Magurele, Judecatoria Targu Secuiesc, Judecatoria Targu Jiu, Judecatoria Targu Carbunesti, Judecatoria Targoviste, Judecatoria Strehaia, Judecatoria Slobozia, Judecatoria Slatina, Judecatoria Sinaia, Judecatoria Sibiu, Judecatoria Sfantu Gheorghe, Judecatoria Segarcea, Judecatoria Sebes, Judecatoria Satu Mare, Judecatoria Saliste, Judecatoria Rupea, Judecatoria Ramnicu Sarat, Judecatoria Raducaneni, Judecatoria Racari, Judecatoria Pucioasa, Judecatoria Pogoanele, Judecatoria Ploiesti, Judecatoria Petrosani, Judecatoria Patarlagele, Judecatoria Pascani, Judecatoria Orsova, Judecatoria Orastie, Judecatoria Oltenita, Judecatoria Novaci, Judecatoria Negresti Oas, Judecatoria Motru, Judecatoria Moreni, Judecatoria Mizil, Judecatoria Miercurea Ciuc, Judecatoria Mediaș, Judecatoria Lehliu-Gara, Judecatoria Intorsura Buzaului, Judecatoria Iasi, Judecatoria Husi, Judecatoria Hunedoara, Judecatoria Hateg, Judecatoria Harlau, Judecatoria Giurgiu, Judecatoria Galați, Judecatoria Gaesti, Judecatoria Filiasi, Judecatoria Fetesti, Judecatoria Fagaras, Judecatoria Dr Tr Severin, Judecatoria Deva, Judecatoria Craiova, Judecatoria Cornetu, Judecatoria Corabia, Judecatoria Cimpeni, Judecatoria Carei, Judecatoria Caracal, Judecatoria Campina, Judecatoria Calarasi, Judecatoria Calafat, Judecatoria Buzau, Judecatoria Buftea, Judecatoria Brasov, Judecatoria Brad, Judecatoria Bolintin Vale, Judecatoria Blaj, Judecatoria Barlad, Judecatoria Bals, Judecatoria Bailesti, Judecatoria Baia de Arama, Judecatoria Avrig, Judecatoria Alexandria, Judecatoria Alba Iulia, Judecatoria Aiud, Judecatoria Agnita, Judecatori Rosiori de Vede, Inalta Curte de Casatie si Justitie, Curtea de Apel Târgu-Mureș, Curtea de Apel Timișoara, Curtea de Apel Suceava, Curtea de Apel Ploiești, Curtea de Apel Oradea, Curtea de Apel Iasi, Curtea de Apel Galați, Curtea de Apel Craiova, Curtea de Apel Constanța, Curtea de Apel Bucuresti, Curtea de Apel Brasov, Curtea de Apel Alba Iulia, Curtea Militară de Apel București,

Momentan cunoastem doar Curtea de Apel Cluj, care foloseste alt sistem, insa care are propriile vulnerabilitati, desi in opinia noastra mai putin severe in mod individual. Vom detalia infra.

Datele detinatorilor sunt accesibile pe portalul instantelor de judecata “https://portal.just.ro/SitePages/acasa.aspx”.

Este notabil insa ca printre ele se afla si instante miltare, care cel mai probabil ar trebui sa se bucure de un sistem de autentificare in 2 pasi, sau care in orice caz sa verifice in doua moduri identitatea partilor.

Un grad similar de risc apare in spetele judecate de ICCJ, care include spete care tin de siguranta nationala, si care, in contextul in care informatiile ar putea fi obtinute printr-o cautare secventiala a numarului documentelor, intr-o seara, ar putea genera probleme semnificative.

In timp ce din ratiuni logice, informatiile secrete, a caror acces este restrictionat in baza unor certificari (precum ORNISS), cel mai probabil **nu se regasesc** pe dosarul electronic, e posibil ca alte informatii cel putin sensibile sa fie totusi accesibile.

De aceea, recomandam implementarea unui sistem bazat pe nivelul de sensibilitate, posibil autentificare intr-un singur pas pentru link-urile simple (cod email), si autentificare in 2 pasi pentru conturile care deja beneficiaza de un cont pe dosarul electronic.

La prima autentificare in dosar, justitiabilii ar trebui sa primeasca prompt-ul de a activa autentificarea in mai multi pasi, ca ulterior sa seteze o parola puternica.

O implementare mai favorabila ar fi prin implementarea proiectului "**ROeID**", dezvoltat de "**Autoritatea pentru Digitalizarea Romaniei**", care este disponibil institutiilor publice si foloseste un sistem biometric de verificare a identitatii.

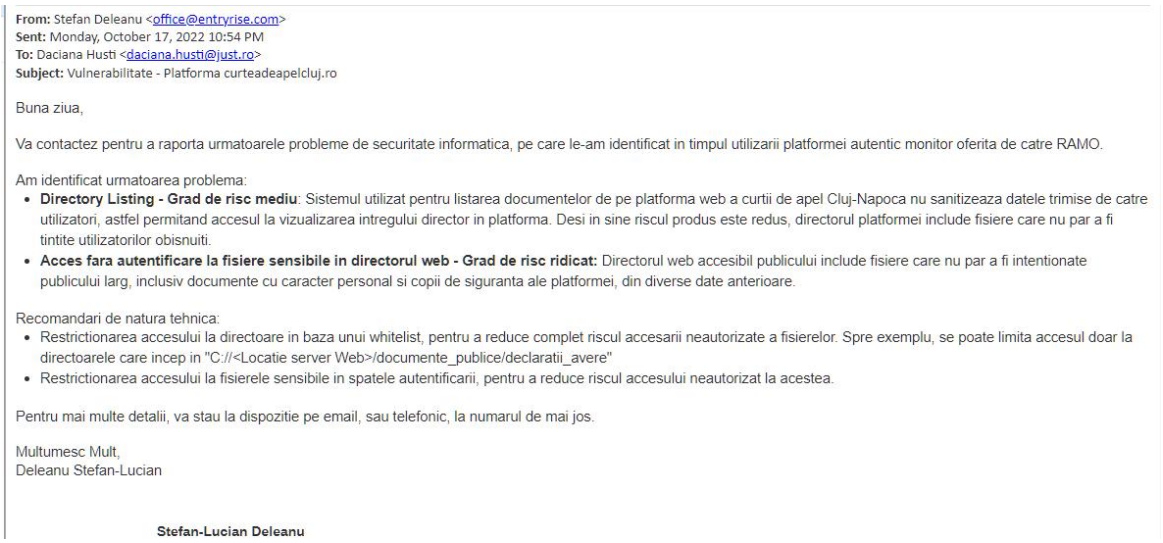
In viitor, presupunem ca ROeID va implementa inrolarea cu cartile de identitate electronice, prin scanarea NFC, si ulterior implementarea, prin sistemul unic de autentificare, al unui sistem OAuth.

APLICATIE “CURTEA DE APEL CLUJ”

Pe data de Octombrie 17, 2022, am identificat prima data o vulnerabilitate de directory listing & traversal, pe endpoint-ul de afisare a fisierelor (eg: documentelor) al platformei Curtii de Apel Cluj.

Suplimentar, lipsea autentificarea sau blocarea accesarii de fisiere sau foldere sensibile, precum:

- Backup numit “ECRISS” - probabil backup sistem, care include si date de autentificare,
- Backup-uri wordpress
- certificat VPN (pt server vpn curtea de apel)
- Backup-uri sistemul curtii de apel (posibil daca era verificat erau vulnerabilitati si in sistemul de dosare al curtii de apel Cluj, separat de cel descris supra)



From: Stefan Deleanu <office@entryrise.com>
Sent: Monday, October 17, 2022 10:54 PM
To: Daciana Husti <daciana.husti@just.ro>
Subject: Vulnerabilitate - Platforma curteadeapelcluj.ro

Buna ziua,

Va contactez pentru a raporta urmatoarele probleme de securitate informatica, pe care le-am identificat in timpul utilizarii platformei autentic monitor oferita de catre RAMO.

Am identificat urmatoarea problema:

- **Directory Listing - Grad de risc mediu**: Sistemul utilizat pentru listarea documentelor de pe platforma web a curtii de apel Cluj-Napoca nu sanitizeaza datele trimise de catre utilizatori, astfel permitand accesul la vizualizarea intregului director in platforma. Desi in sine riscul produs este redus, directorul platformei include fisiere care nu par a fi tintite utilizatorilor obisnuiti.
- **Acces fara autentificare la fisiere sensibile in directorul web - Grad de risc ridicat:** Directorul web accesibil publicului include fisiere care nu par a fi intentionate publicului larg, inclusiv documente cu caracter personal si copii de siguranta ale platformei, din diverse date anterioare.

Recomandari de natura tehnica:

- Restrictionarea accesului la directoare in baza unui whitelist, pentru a reduce complet riscul accesarii neautorizate a fisierelor. Spre exemplu, se poate limita accesul doar la directoarele care incep in "C://<Locatie server Web>/documente_publice/declaratii_avere"
- Restrictionarea accesului la fisierele sensibile in spatele autentificarii, pentru a reduce riscul accesului neautorizat la acestea.

Pentru mai multe detalii, va stau la dispozitie pe email, sau telefonic, la numarul de mai jos.

Multumesc Mult,
Deleanu Stefan-Lucian

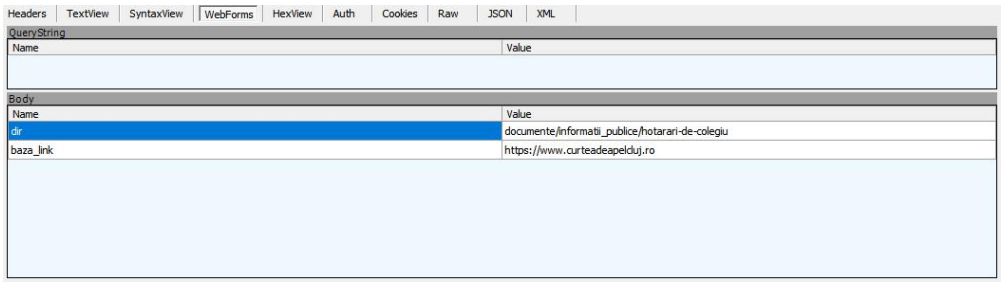
Stefan-Lucian Deleanu

Pe data de Octombrie 19, 2022, am fost notificati ca s-au remediat, si am primit solicitarea de a continua raportarea de vulnerabilitati.

Insa, am identificat in mod curent ca vulnerabilitatea persista. Pentru a reproduce vulnerabilitatea:

1. Accesarea oricarei liste de fisiere (eg: Hotarari de colegiu): https://www.curteadeapelcluj.ro/index.php/informatii-publice/hotarari-de-colegiu.html

Se poate folosi fiddler pentru a observa ca in verificarea listei de fisiere, se trimite un request POST catre urmatorul endpoint: “https://www.curteadeapelcluj.ro/Foldertree_hotarari_colegiu.php”, al carei valoare de “dir” si baza_link se pot modifica de la:



Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

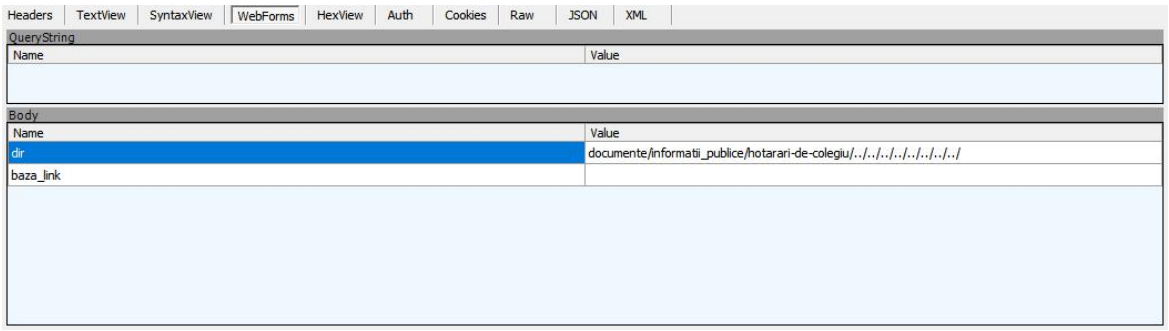
QueryString

Name	Value

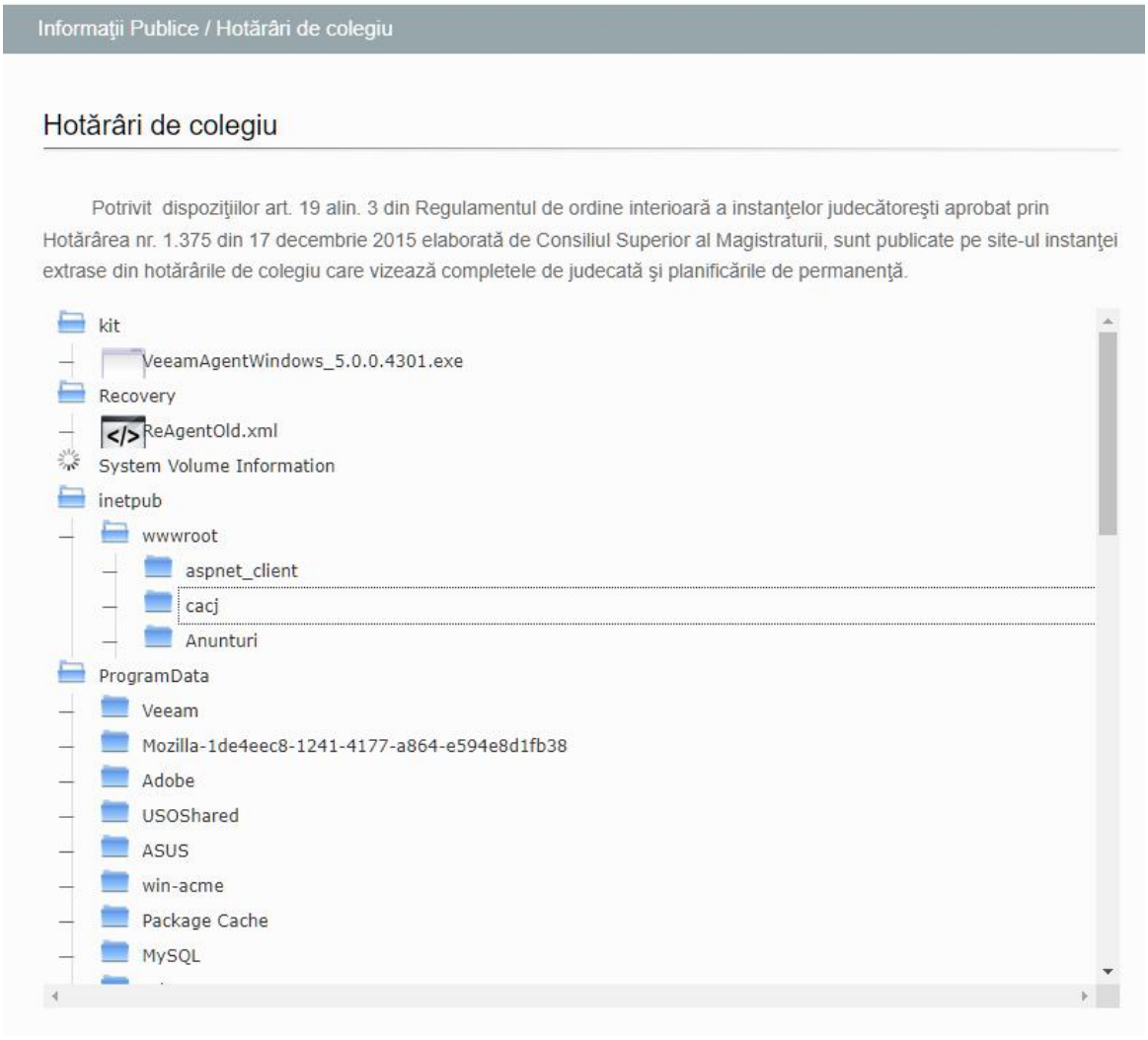
Body

Name	Value
dir	documente/informatii_publice/hotarari-de-colegiu
baza_link	https://www.curteadeapelcluj.ro

La:



Pentru a putea vizualiza toate fisierele din partitia C:/



In timp ce intr-adevar, acum s-au blocat descarcarile pe anumite URL-uri, unele au ramas uitate (eg: ai1wm-backups) unde se poate descarca un backup din 2023.11.13 al curtii de apel, in format “wpress”.

Aceste backup-uri par sa fie cu un anumit grad de periodicitate, cea ce implica riscul ca un atacator sa poata obtine acces la backup, astfel la baza de date, si de acolo, la sesiunea unui user (sau un cont

prost parolat), pe care sa il foloseasca pentru a introduce un plugin de Wordpress cu care sa aiba ulterior acces shell cu un PHP shell sau ASPX shell.

APLICATIE WEB “bibnat.ro”

Biblioteca nationala a Romaniei a fost identificata relativ recent ca are o vulnerabilitate in modul in care sanitizeaza fisierele uploadate prin diversele formulare de pe site, pentru ca am putut uploada fisiere .png cu marimi enorme, lucru ce a demonstrat ca fisierele sunt uploadate fara a fi modificate.

https://bibnat.ro/ISSN-s122-ro.htm

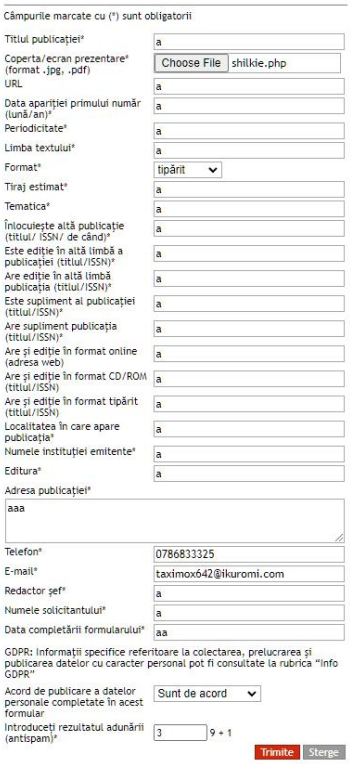
La validarea existentei unei astfel de lipse de sanitizare, s-a identificat bresa prin uploadarea unui fisier php tip shell. Evident s-a adeverit existenta vulnerabilitatii:

Pentru validare, a se uploada un shell php script sau un info.php, pe diversele formulare ale BIBNAT, cu un email valid.

Se va primi un link cu adresa unde a fost stocat shell script-ul.

Am notificat biblioteca nationala, au sters fisierul shell, si ne-au notificat ca “vor tine cont in constructia noului site de aceste tipuri de vulnerabilitati”, deci cu 0 interes.

Prin vulnerabilitatea mentionata se poate accesa toate functiile prin platforma WEB a bibliotecii nationale.



Se introduc valori arbitrare in toate field-urile cu exceptia celui de upload, unde se pot uploada fisiere php.

Se termina captcha-ul, se trimite. Se va primi pe mail-ul atasat link-ul cu shell-ul.

Nu au dezactivat nici executia de programe din php, desi li s-a subliniat riscul.