Divulgation responsable

Investment Publishing International BV, l'éditeur d'*Investment Officer*, fait partie de FD Mediagroep. FDMediagroep accorde une grande importance à la sécurité de ses systèmes. Malgré le soin que nous y apportons, des vulnérabilités peuvent toutefois toujours exister.

Si vous avez découvert une vulnérabilité dans l'un de nos systèmes, nous souhaitons en être informés afin de pouvoir prendre des mesures le plus rapidement possible. Nous accordons une grande importance à une approche collaborative, en vue de mieux protéger nos clients et nos systèmes.

NB : Cette politique de divulgation responsable s'applique uniquement aux systèmes appartenant à des domaines se terminant par :

- `.nl`
- `.be`
- `.lu`
- `.fr`
- `.de`
- `.com`

Les autres domaines ou infrastructures n'entrent pas dans le champ d'application de cette politique.

Nous vous demandons :

- D'envoyer vos résultats par e-mail à security@investmentofficer.com ;
- De ne pas exploiter le problème, par exemple en téléchargeant plus de données que nécessaire pour démontrer la fuite ou en accédant à des données de tiers, en les supprimant ou en les modifiant ;
- De ne pas informer d'autres personnes du problème tant qu'il n'est pas résolu et de supprimer toutes les données confidentielles obtenues grâce à la fuite dès que le problème a été résolu ;
- De ne pas utiliser d'attaques de sécurité physique, d'ingénierie sociale, de déni de service distribué, de spam ou d'applications tierces ; et
- De fournir des informations suffisantes pour reproduire le problème afin que nous puissions le résoudre le plus rapidement possible. En général, l'adresse IP ou l'URL du système affecté et une description de la vulnérabilité suffisent, mais d'autres informations peuvent être nécessaires pour des vulnérabilités plus complexes.
- D'indiquer le numéro CVE de la vulnérabilité dans l'e-mail.

Nous nous engageons à :

- Répondre au rapport dans un délai de 5 jours ;
- Ne pas engager d'action en justice concernant le rapport si vous avez respecté les conditions susmentionnées ;
- Traiter votre rapport de manière confidentielle et ne pas partager vos données personnelles avec des tiers sans votre consentement, à moins que cela ne soit nécessaire pour nous conformer à une obligation légale. Le signalement peut être fait sous un pseudonyme ;
- Vous tenir informé de l'évolution de la résolution du problème,
- Mentionner, si vous le souhaitez, votre nom en tant que découvreur lorsque nous vous informons du problème signalé. En guise de remerciement pour votre aide, nous offrirons une récompense pour chaque signalement d'un problème de sécurité dont nous n'avons pas encore connaissance. Nous déterminerons le montant de la récompense en fonction de la gravité de la fuite et de la qualité du rapport, avec un minimum de 50 euros. Nous aurons besoin d'une facture pour le paiement. S'il n'est pas possible d'envoyer une facture, nous envisagerons d'offrir un bon d'achat en guise d'alternative.

Nous nous efforçons de résoudre tous les problèmes le plus rapidement possible et nous serions ravis de participer à toute publication concernant le problème après qu'il a été résolu.
FDMG peut décider qu'une vulnérabilité potentielle présentant un risque faible ou accepté ne sera pas récompensée. Voici quelques exemples de vulnérabilités hors du champ d'application :

- Codes HTTP 404 ou autres codes non HTTP 200
- Insertion de texte en clair dans les pages 404
- Bannières de version sur les services publics
- Fichiers et dossiers accessibles au public contenant des informations non sensibles
- Détournement de clics sur des pages sans fonction de connexion
- Falsification des requêtes intersites (CSRF) sur les formulaires accessibles de manière anonyme
- Absence d'indicateurs « sécurisé »/« HTTP uniquement » sur les cookies non sensibles
- Utilisation de la méthode HTTP OPTIONS
- Injection d'en-tête d'hôte
- Absence d'enregistrements SPF, DKIM et DMARC
- DNSSEC manquant
- En-têtes de sécurité HTTP manquants ou mal appliqués, tels que :
    - Strict Transport Security (HSTS)
    - HTTP Public Key Pinning (HPKP)
    - Content Security Policy (CSP)
    - X-Content-Type-Option
    - X-Frame-Option
    - X-WebKit CSP
    - X-XSS-Protection