trading.com

POLITIQUE DE DIVULGATION RESPONSABLE

1. INTRODUCTION

Trading.com Markets EU Ltd (ci-après « Trading.com ») reconnaît la nécessité de se rapprocher de la communauté de la cybersécurité afin de protéger les données de ses clients et de collaborer à la création de solutions et d'applications plus sécurisées. La présente politique vise à fournir aux chercheurs en sécurité des directives claires pour mener leurs activités de recherche de vulnérabilités et à leur indiquer la manière dont nous préférons qu'ils nous signalent les vulnérabilités découvertes.

Les chercheurs sont invités à signaler volontairement les vulnérabilités qu'ils peuvent trouver en rapport avec les systèmes de Trading.com. Cette politique décrit les systèmes et les types de recherche couverts par cette politique et la manière de nous soumettre des rapports de vulnérabilité.

La soumission de rapports de vulnérabilité est soumise aux conditions générales énoncées sur cette page. En soumettant un rapport de vulnérabilité à Trading.com, les chercheurs reconnaissent avoir lu et accepté ces conditions générales.

2. CONDITIONS GÉNÉRALES

2.1. Sphère de sécurité / Autorisation

Lorsque vous menez des recherches sur les vulnérabilités en faisant preuve de bonne foi pour vous conformer à la présente politique, nous considérons que vos recherches sont :

- Autorisées, conformément à toutes les lois anti-piratage applicables, et nous ne recommanderons ni n'engagerons de poursuites judiciaires à votre encontre pour vos recherches.
- Autorisées en vertu de toute loi anti-contournement pertinente et nous n'engagerons aucune poursuite à votre encontre pour contournement des contrôles technologiques.
- Légales, utiles à la sécurité globale de l'Internet et menées de bonne foi.

Vous êtes tenu de vous conformer à toutes les lois applicables. Si une action en justice est intentée par un tiers à votre encontre pour des activités que vous avez menées de bonne foi conformément à la présente politique, nous ferons connaître cette autorisation.
Si, à tout moment, vous avez des doutes ou des incertitudes quant à la conformité de vos recherches en matière de sécurité avec la présente politique, veuillez soumettre un rapport via l'un de nos canaux officiels (tels que définis ci-dessous) avant de poursuivre.
Veuillez noter que la sphère de sécurité s'applique uniquement aux réclamations légales relevant du contrôle de l'organisation participant à la présente politique et que celle-ci ne lie pas les tiers indépendants.

2.2. Directives

Dans le cadre de la présente politique, le terme « recherche » désigne les activités dans lesquelles vous :

- Nous informez dès que possible après avoir découvert un problème de sécurité réel ou potentiel.
- Faites tout votre possible pour éviter les violations de la vie privée, la dégradation de l'expérience utilisateur, la perturbation des systèmes de production et la destruction ou la manipulation des données.
- N'utilisez les exploits que dans la mesure nécessaire pour confirmer la présence d'une vulnérabilité. N'utilisez pas d'exploit pour compromettre ou exfiltrer des données, établir un accès persistant à la ligne de commande ou utiliser l'exploit pour pivoter vers d'autres systèmes.

trading.com Markets EU Ltd
13 Irenes Street, 3042 Limassol, Chypre
support.eu@trading.com
www.trading.com/eu

Vous êtes également tenu de :

- Respecter les règles, y compris la présente politique et tout autre accord pertinent. En cas de contradiction entre la présente politique et toute autre condition applicable, les conditions de la présente politique prévaudront.
- N'interagir qu'avec vos propres comptes de test.
- Limiter la création de comptes à deux (2) comptes au total pour tous les tests.
- N'utiliser que les canaux officiels pour divulguer et/ou discuter avec nous des informations relatives aux vulnérabilités.
- Soumettre une seule vulnérabilité par rapport, sauf si vous devez enchaîner plusieurs vulnérabilités pour démontrer leur impact.
- Supprimez de manière sécurisée toutes les données récupérées au cours de la recherche une fois le rapport soumis.
- Effectuez les tests uniquement sur les systèmes concernés et respectez les systèmes et activités qui ne sont pas concernés.
- Évitez d'utiliser des outils de scan invasifs ou automatisés à haute intensité pour trouver des vulnérabilités.
- Ne divulguez aucune vulnérabilité sans l'accord écrit préalable de Trading.com.
- N'effectuez aucune attaque par « déni de service ».
- N'effectuez pas d'attaques d'ingénierie sociale et/ou de sécurité physique contre les bureaux, les utilisateurs ou les employés de Trading.com.
- N'effectuez pas de tests automatisés/scriptés sur les formulaires Web, en particulier les formulaires « Contactez-nous » destinés à permettre aux clients de contacter notre service clientèle.

Une fois que vous avez établi l'existence d'une vulnérabilité ou que vous avez accidentellement découvert des données sensibles (y compris des informations personnelles identifiables (PII), des informations financières, des informations exclusives ou des secrets commerciaux de toute partie), **vous devez interrompre votre test, nous en informer immédiatement et ne divulguer ces données à personne d'autre**. Vous devez également limiter votre accès aux données minimales nécessaires pour démontrer efficacement la validité du concept.

2.3. Signalement d'une vulnérabilité / Canaux officiels

Veuillez signaler toute vulnérabilité à vulnerability.disclosure.eu@trading.com en fournissant toutes les informations pertinentes. Afin d'accélérer la vérification de votre découverte, veuillez fournir les informations suivantes dans votre premier message :

- Emplacement, URL ou chemin d'accès à l'application où la vulnérabilité a été découverte.
- Description de la vulnérabilité et de l'impact potentiel de son exploitation.
- Instructions pour reproduire la vulnérabilité (il peut s'agir d'étapes écrites, d'une vidéo ou d'une série de captures d'écran détaillant la preuve de concept)
- L'adresse e-mail, l'agent utilisateur et le(s) nom(s) d'utilisateur utilisé(s) sur la plateforme de trading (le cas échéant).
- Votre clé publique PGP pour permettre une communication cryptée (si disponible).

2.4. Portée

(a) Systèmes/services concernés

trading.com Markets EU Ltd
13 Irenes Street, 3042 Limassol, Chypre
support.eu@trading.com
www.trading.com/eu

Domaines	www.trading.com/eu/
Application Android	Application officielle trading.com (com.trading.application)
Application iOS	Application officielle trading.com (id1576478434)

(b) Systèmes/services hors portée

Tout service (tel que les services connectés), système ou domaine qui n'est pas expressément mentionné dans la section « Systèmes/services concernés » ci-dessus est exclu du champ d'application et n'est pas autorisé à faire l'objet de tests. En outre, les vulnérabilités découvertes dans les systèmes de nos fournisseurs ne relèvent pas du champ d'application de la présente politique et doivent être signalées directement au fournisseur conformément à sa politique de divulgation (le cas échéant). Si vous ne savez pas si un système est concerné ou non, contactez-nous à l'adresse vulnerability.disclosure.eu@trading.com .

(c) Vulnérabilités concernées

- Injection SQL
- Script inter-sites (XSS)
- Exécution de code à distance (RCE)
- Falsification de requêtes côté serveur (SSRF)
- Authentification et gestion de session défaillantes
- Référence directe non sécurisée à un objet (IDOR)
- Exposition de données sensibles
- Traversée de répertoires/chemins
- Inclusion de fichiers locaux/distants
- Falsification de requêtes intersites (CSRF) avec un impact démontrable élevé
- Redirection ouverte sur des paramètres sensibles
- Prise de contrôle du sous-domaine (pour la prise de contrôle du sous-domaine, ajoutez un message convivial tel que : « Nous travaillons sur le problème et nous serons de retour bientôt. »)

(d) Vulnérabilités hors portée

Certaines vulnérabilités sont considérées comme hors du portée d'application du programme de divulgation des vulnérabilités. Ces vulnérabilités hors du champ d'application comprennent, sans s'y limiter :

- Problèmes de configuration de la messagerie, notamment les paramètres SPF, DKIM et DMARC
- Vulnérabilités de type « clickjacking » qui ne conduisent pas à des actions sensibles, telles que la modification d'un compte
- Self-XSS (c'est-à-dire lorsqu'un utilisateur doit être incité à coller du code dans son navigateur web)
- Usurpation de contenu dont l'impact est minime (par exemple, injection de texte non HTML)
- Falsification de requêtes intersites (CSRF) dont l'impact est minime (par exemple, CSRF dans les formulaires de connexion ou de déconnexion)
- Redirection ouverte, sauf si un impact supplémentaire sur la sécurité peut être démontré
- Attaques CRLF dont l'impact est minime
- Injection d'en-tête d'hôte lorsque l'impact est minime

trading.com Markets EU Ltd
13 Irenes Street, 3042 Limassol, Chypre
support.eu@trading.com
www.trading.com/eu

- Absence des indicateurs *HttpOnly* ou *Secure* sur les cookies non sensibles
- Absence de bonnes pratiques dans la configuration SSL/TLS et les chiffrements
- En-têtes de sécurité HTTP manquants ou mal configurés (par exemple, CSP, HSTS)
- Formulaires sans contrôles Captcha
- Énumération des noms d'utilisateur/adresses e-mail via le message d'erreur de la page de connexion
- Énumération des noms d'utilisateur/adresses e-mail via le message d'erreur « Mot de passe oublié »
- Problèmes nécessitant une interaction peu probable de l'utilisateur
- Complexité du mot de passe ou tout autre problème lié aux politiques relatives aux comptes ou aux mots de passe
- Absence de délai d'expiration de session
- Attaques par force brute
- Problèmes de limite de fréquence pour les actions non critiques
- Vulnérabilités WordPress sans preuve d'exploitabilité
- Divulgation de versions vulnérables de logiciels sans preuve d'exploitabilité
- Toute activité susceptible d'entraîner une interruption de notre service (DoS)
- Absence de protection root / Contournement de la protection root (applications mobiles)
- Absence de certificat SSL / Contournement du certificat SSL (applications mobiles)
- Absence d'obfuscation du code (applications mobiles)

2.5. Dépannage et délais de réponse

L'équipe de sécurité accusera réception de votre rapport dans un délai de trois jours ouvrables. Nous travaillerons avec les équipes internes pour vérifier les conclusions et vous répondre dans les meilleurs délais avec une mise à jour ou une demande d'informations supplémentaires.

Si la découverte soumise est confirmée comme valide, l'équipe de sécurité procédera à la correction ou à l'atténuation du problème en fonction de son impact et de sa gravité. Nous nous efforcerons de vous tenir informé de l'avancement du processus.

3. RÉCOMPENSES

Nous apprécions le temps et les efforts consacrés à signaler les failles de sécurité conformément à la présente politique. Cependant, nous n'offrons actuellement aucune récompense pour la divulgation de failles. Cette politique est susceptible d'être modifiée à l'avenir.

4. DÉTAILS DE LA CLÉ PGP

Nous encourageons les personnes qui signalent des vulnérabilités à utiliser des canaux de communication cryptés afin de protéger la confidentialité de leurs rapports à l'aide de notre clé publique PGP.
Empreinte digitale de la clé PGP : 2F2F9F5449F1F649804F9B7F297F8FD1B8048BCD
Télécharger la clé PGP
Remarque : veuillez crypter vos messages à l'aide de la clé PGP ci-dessus et inclure votre propre clé publique dans l'e-mail.

5. COMMENTAIRES

trading.com Markets EU Ltd
13 Irenes Street, 3042 Limassol, Chypre
support.eu@trading.com
www.trading.com/eu

Si vous souhaitez nous faire part de vos commentaires ou suggestions concernant cette politique, veuillez nous contacter à l'adresse vulnerability.disclosure.eu@trading.com .
Merci de contribuer à la sécurité de Trading.com et de ses utilisateurs.

trading.com Markets EU Ltd
13 Irenes Street, 3042 Limassol, Chypre
support.eu@trading.com
www.trading.com/eu