trading.com

VERANTWORTUNGSBEWUSSTE OFFENLEGUNGSPOLITIK

1. EINLEITUNG

Trading.com Markets EU Ltd (im Folgenden „Trading.com“) erkennt die Notwendigkeit an, sich an die Cybersicherheits-Community zu wenden, um Kundendaten zu schützen und gemeinsam sicherere Lösungen und Anwendungen zu entwickeln. Diese Richtlinie soll Sicherheitsforschern klare Richtlinien für die Durchführung von Aktivitäten zur Aufdeckung von Schwachstellen geben und unsere Präferenzen hinsichtlich der Übermittlung entdeckter Schwachstellen an uns darlegen.

Forscher sind herzlich eingeladen, Schwachstellen, die sie im Zusammenhang mit den Systemen von Trading.com finden, freiwillig zu melden. Diese Richtlinie beschreibt, welche Systeme und Arten von Forschung unter diese Richtlinie fallen und wie Schwachstellenberichte an uns übermittelt werden können.

Die Übermittlung von Berichten über Sicherheitslücken unterliegt den auf dieser Seite aufgeführten Bedingungen. Mit der Übermittlung eines Berichts über eine Sicherheitslücke an Trading.com bestätigen die Forscher, dass sie diese Bedingungen gelesen und akzeptiert haben.

2. ALLGEMEINE GESCHÄFTSBEDINGUNGEN

2.1. Safe Harbor / Genehmigung

Wenn Sie bei der Durchführung von Sicherheitsrecherchen in gutem Glauben bemüht sind, diese Richtlinie einzuhalten, betrachten wir Ihre Recherche als

- Autorisiert in Bezug auf alle geltenden Anti-Hacking-Gesetze, und wir werden keine rechtlichen Schritte gegen Sie wegen Ihrer Forschung empfehlen oder einleiten.
- Als autorisiert in Bezug auf alle relevanten Gesetze zur Umgehung von Sicherheitsvorkehrungen, und wir werden keine Ansprüche gegen Sie wegen Umgehung von technischen Kontrollen geltend machen.
- rechtmäßig, hilfreich für die allgemeine Sicherheit des Internets und in gutem Glauben durchgeführt.

Von Ihnen wird erwartet, dass Sie alle geltenden Gesetze einhalten. Wenn Dritte rechtliche Schritte gegen Sie wegen Aktivitäten einleiten, die Sie in gutem Glauben und in Übereinstimmung mit dieser Richtlinie durchgeführt haben, werden wir diese Genehmigung bekannt geben.
Wenn Sie zu irgendeinem Zeitpunkt Bedenken haben oder unsicher sind, ob Ihre Sicherheitsrecherchen mit dieser Richtlinie vereinbar sind, reichen Sie bitte einen Bericht über einen unserer offiziellen Kanäle (wie unten angegeben) ein, bevor Sie weitere Schritte unternehmen.
Beachten Sie, dass Safe Harbor nur für Rechtsansprüche gilt, die der Kontrolle der an dieser Richtlinie beteiligten Organisation unterliegen, und dass die Richtlinie keine unabhängigen Dritten bindet.

2.2. Richtlinien

Im Rahmen dieser Richtlinie bezeichnet „Recherche“ Aktivitäten, bei denen Sie:

- Sie uns so schnell wie möglich benachrichtigen, nachdem Sie ein tatsächliches oder potenzielles Sicherheitsproblem entdeckt haben.
- alle Anstrengungen unternehmen, um Datenschutzverletzungen, Beeinträchtigungen der Benutzererfahrung, Störungen der Produktionssysteme sowie die Zerstörung oder Manipulation von Daten zu vermeiden
- Exploits nur in dem Umfang verwenden, der zur Bestätigung des Vorhandenseins einer Schwachstelle erforderlich ist. Keine Exploits verwenden, um Daten zu kompromittieren oder zu

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

exfiltrieren, einen dauerhaften Befehlszeilenzugriff einzurichten oder den Exploit zu nutzen, um auf andere Systeme zuzugreifen.

Darüber hinaus werden Sie gebeten

- die Regeln einzuhalten, einschließlich dieser Richtlinie und aller anderen relevanten Vereinbarungen. Bei Widersprüchen zwischen dieser Richtlinie und anderen geltenden Bestimmungen gelten die Bestimmungen dieser Richtlinie.
- Interagieren Sie nur mit Ihren eigenen Testkonten.
- Beschränken Sie die Erstellung von Konten auf insgesamt zwei (2) Konten für alle Tests.
- Verwenden Sie nur die offiziellen Kanäle, um Schwachstelleninformationen an uns weiterzugeben und/oder mit uns zu besprechen.
- Reichen Sie pro Bericht nur eine Sicherheitslücke ein, es sei denn, Sie müssen mehrere Sicherheitslücken miteinander verknüpfen, um die Auswirkungen zu demonstrieren.
- Löschen Sie alle während der Untersuchung abgerufenen Daten sicher, sobald der Bericht übermittelt wurde.
- Führen Sie Tests nur auf Systemen durch, die zum Umfang gehören, und respektieren Sie Systeme und Aktivitäten, die nicht zum Umfang gehören.
- Vermeiden Sie den Einsatz intensiver invasiver oder automatisierter Scan-Tools, um Schwachstellen zu finden.
- Geben Sie keine Sicherheitslücken ohne vorherige schriftliche Zustimmung von Trading.com öffentlich bekannt.
- Führen Sie keine „Denial of Service"-Angriffe durch.
- Führen Sie keine Social-Engineering- und/oder physischen Sicherheitsangriffe auf die Büros, Benutzer oder Mitarbeiter von Trading.com durch.
- Führen Sie keine automatisierten/skriptgesteuerten Tests von Webformularen durch, insbesondere nicht von „Kontakt"-Formularen, die für Kunden zur Kontaktaufnahme mit unserem Kundenservice vorgesehen sind.

Sobald Sie festgestellt haben, dass eine Schwachstelle besteht, oder Sie unbeabsichtigt auf sensible Daten (einschließlich personenbezogener Daten (PII), Finanzinformationen oder geschützte Informationen oder Geschäftsgeheimnisse einer Partei) stoßen, **müssen Sie Ihren Test beenden, uns unverzüglich benachrichtigen und diese Daten nicht an Dritte weitergeben**. Sie sollten Ihren Zugriff auch auf die Daten beschränken, die für einen wirksamen Nachweis des Konzepts erforderlich sind.

2.3. Meldung einer Sicherheitslücke / Offizielle Kanäle

Bitte melden Sie alle Sicherheitslücken unter vulnerability.disclosure.eu@trading.com und geben Sie dabei alle relevanten Informationen an. Um die Überprüfung Ihrer Feststellung zu beschleunigen, geben Sie bitte in Ihrer ersten Mitteilung die folgenden Informationen an:

- Ort, URL oder Anwendungspfad, an dem die Sicherheitslücke entdeckt wurde.
- Beschreibung der Sicherheitslücke und der potenziellen Auswirkungen einer Ausnutzung.
- Anweisungen zur Reproduktion der Sicherheitslücke (dies können schriftliche Schritte, ein Video oder eine Reihe von Screenshots sein, die den Proof-of-Concept detailliert beschreiben)
- Die E-Mail-Adresse, der User-Agent und die Benutzernamen, die auf der Handelsplattform verwendet werden (falls vorhanden).
- Ihre öffentliche PGP-Schlüssel, um eine verschlüsselte Kommunikation zu ermöglichen (falls verfügbar).

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

2.4. Bewertung

(a) Betroffene Systeme/Dienste

Domains	www.trading.com/eu/
Android-App	Offizielle trading.com-App (com.trading.application)
iOS-App	Offizielle App von trading.com (id1576478434)

(b) Nicht abgedeckte Systeme/Dienste

Alle Dienste (z. B. verbundene Dienste), Systeme oder Domänen, die nicht ausdrücklich im Abschnitt „In den Geltungsbereich fallende Systeme/Dienste" oben aufgeführt sind, sind vom Geltungsbereich ausgeschlossen und dürfen nicht getestet werden. Darüber hinaus fallen Schwachstellen, die in Systemen unserer Lieferanten gefunden werden, nicht in den Geltungsbereich dieser Richtlinie und sollten gemäß den Offenlegungsrichtlinien des Lieferanten (sofern vorhanden) direkt an diesen gemeldet werden. Wenn Sie sich nicht sicher sind, ob ein System in den Geltungsbereich fällt, wenden Sie sich bitte anvulnerability.disclosure.eu@trading.com .

(c) Sicherheitslücken im Geltungsbereich

- SQL-Injection
- Cross-Site-Scripting (XSS)
- Remote-Code-Ausführung (RCE)
- Server-Side Request Forgery (SSRF)
- Fehlerhafte Authentifizierung und Sitzungsverwaltung
- Unsichere direkte Objektreferenz (IDOR)
- Offenlegung sensibler Daten
- Verzeichnis-/Pfad-Traversal
- Lokale/Remote-Datei-Einbindung
- Cross-Site-Request-Forgery (CSRF) mit nachweislich hoher Auswirkung
- Offene Weiterleitung bei sensiblen Parametern
- Übernahme von Subdomains (Fügen Sie bei der Übernahme von Subdomains eine freundliche Meldung hinzu, z. B.: „Wir arbeiten daran und sind bald wieder verfügbar.")

(d) Nicht abgedeckte Schwachstellen

Bestimmte Schwachstellen gelten als außerhalb des Geltungsbereichs des Schwachstellenmeldungsprogramms. Zu diesen Schwachstellen gehören unter anderem:

- Probleme mit der E-Mail-Konfiguration, einschließlich SPF-, DKIM- und DMARC-Einstellungen
- Clickjacking-Schwachstellen, die nicht zu sensiblen Aktionen wie der Änderung von Konten führen
- Self-XSS (d. h. wenn ein Benutzer dazu verleitet werden muss, Code in seinen Webbrowser einzufügen)
- Content-Spoofing, bei dem die Auswirkungen minimal sind (z. B. Einfügen von Nicht-HTML-Text)
- Cross-Site Request Forgery (CSRF), bei der die Auswirkungen minimal sind (z. B. CSRF in Anmelde- oder Abmeldeformularen)

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

- Offene Weiterleitung – es sei denn, es kann eine zusätzliche Sicherheitsauswirkung nachgewiesen werden
- CRLF-Angriffe, bei denen die Auswirkungen minimal sind
- Host-Header-Injektion, bei der die Auswirkungen minimal sind
- Fehlende *HttpOnly*- oder Secure-Flags bei nicht sensiblen Cookies
- Fehlende Best Practices bei der SSL/TLS-Konfiguration und Verschlüsselung
- Fehlende oder falsch konfigurierte HTTP-Sicherheitsheader (z. B. CSP, HSTS)
- Formulare ohne Captcha-Kontrollen
- Aufzählung von Benutzernamen/E-Mail-Adressen über Fehlermeldung auf der Anmeldeseite
- Aufzählung von Benutzernamen/E-Mail-Adressen über Fehlermeldung „Passwort vergessen“
- Probleme, die eine unwahrscheinliche Benutzerinteraktion erfordern
- Komplexität des Passworts oder andere Probleme im Zusammenhang mit Konto- oder Passwortrichtlinien
- Fehlende Sitzungszeitüberschreitung
- Brute-Force-Angriffe
- Rate-Limit-Probleme für nicht kritische Aktionen
- WordPress-Sicherheitslücken ohne Nachweis der Ausnutzbarkeit
- Offenlegung einer anfälligen Softwareversion ohne Nachweis der Ausnutzbarkeit
- Jede Aktivität, die zu einer Störung unseres Dienstes führen könnte (DoS)
- Fehlender Root-Schutz / Umgehung des Root-Schutzes (mobile Anwendungen)
- Fehlende SSL-Zertifikat-Bindung / Umgehung der SSL-Zertifikat-Bindung (mobile Anwendungen)
- Fehlende Code-Verschleierung (mobile Anwendungen)

2.5. Behebung und Reaktionszeiten

Das Sicherheitsteam bestätigt den Eingang Ihrer Meldung innerhalb von drei Werktagen. Wir arbeiten mit internen Teams zusammen, um den Befund zu überprüfen und zeitnah mit einer Aktualisierung oder einer Anfrage nach zusätzlichen Informationen zu reagieren.

Wenn sich die gemeldete Feststellung als gültig bestätigt, wird das Sicherheitsteam je nach Auswirkung und Schweregrad der Feststellung Maßnahmen zur Behebung oder Minderung des Problems ergreifen. Wir werden Sie während des gesamten Prozesses über den aktuellen Stand informieren.

3. BELOHNUNG

Wir schätzen alle, die sich die Zeit und Mühe nehmen, Sicherheitslücken gemäß dieser Richtlinie zu melden. Derzeit bieten wir jedoch keine Belohnungen für die Offenlegung von Sicherheitslücken an. Dies kann sich in Zukunft ändern.

4. PGP-SCHLÜSSELDETAILS

Wir empfehlen Meldenden, zur Wahrung der Vertraulichkeit von Sicherheitslücken verschlüsselte Kommunikationskanäle zu verwenden und unseren öffentlichen PGP-Schlüssel zu nutzen.
PGP-Schlüssel-Fingerabdruck: 2F2F9F5449F1F649804F9B7F297F8FD1B8048BCD
PGP-Schlüssel herunterladen
Hinweis: Bitte verschlüsseln Sie Ihre Nachrichten mit dem oben genannten PGP-Schlüssel und fügen Sie Ihren eigenen öffentlichen Schlüssel in die E-Mail ein.

5. FEEDBACK

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

Wenn Sie Feedback oder Vorschläge zu dieser Richtlinie haben, wenden Sie sich bitte anvulnerability.disclosure.eu@trading.com .
Vielen Dank, dass Sie dazu beitragen, Trading.com und unsere Nutzer zu schützen.

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