

trading.com

POLITICA DI DIVULGAZIONE RESPONSABILE

1. INTRODUZIONE

Trading.com Markets EU Ltd (di seguito "Trading.com") riconosce la necessità di collaborare con la comunità della sicurezza informatica per proteggere i dati dei clienti e lavorare insieme per creare soluzioni e applicazioni più sicure. La presente politica ha lo scopo di fornire ai ricercatori di sicurezza linee guida chiare per lo svolgimento delle attività di individuazione delle vulnerabilità e di comunicare le nostre preferenze in merito alle modalità di segnalazione delle vulnerabilità individuate.

I ricercatori sono invitati a segnalare volontariamente le vulnerabilità che riscontrano nei sistemi di Trading.com. La presente politica descrive quali sistemi e tipi di ricerca sono coperti dalla stessa e come inviarci le segnalazioni di vulnerabilità.

L'invio di segnalazioni di vulnerabilità è soggetto ai termini e alle condizioni stabiliti in questa pagina e, inviando una segnalazione di vulnerabilità a Trading.com, i ricercatori riconoscono di aver letto e accettato tali termini e condizioni.

2. TERMINI E CONDIZIONI

2.1. Safe Harbor / Autorizzazione

Quando conduci una ricerca sulle vulnerabilità, dimostrando un impegno in buona fede a rispettare la presente politica, consideriamo la tua ricerca:

- Autorizzata, in relazione a qualsiasi legge anti-hacking applicabile e non raccomandiamo né intraprenderemo azioni legali nei vostri confronti per la vostra ricerca.
- Autorizzata in relazione a qualsiasi legge anti-elusione pertinente e non intraprenderemo alcuna azione legale nei tuoi confronti per elusione dei controlli tecnologici.
- Legittime, utili alla sicurezza generale di Internet e condotte in buona fede.

L'utente è tenuto a rispettare tutte le leggi applicabili. Se un'azione legale viene avviata da una terza parte nei confronti dell'utente per attività svolte in buona fede in conformità con la presente politica, renderemo nota la presente autorizzazione.

Se in qualsiasi momento avete dubbi o incertezze sulla conformità della vostra ricerca sulla sicurezza alla presente politica, vi preghiamo di inviare una segnalazione tramite uno dei nostri canali ufficiali (come indicato di seguito) prima di procedere.

Si noti che Safe Harbor si applica solo alle rivendicazioni legali sotto il controllo dell'organizzazione che partecipa alla presente politica e che la politica non vincola terze parti indipendenti.

2.2. Linee guida

Ai sensi della presente politica, per "ricerca" si intendono le attività in cui l'utente:

- Ci informi il prima possibile dopo aver scoperto un problema di sicurezza reale o potenziale.
- Fate ogni sforzo per evitare violazioni della privacy, degrado dell'esperienza utente, interruzione dei sistemi di produzione e distruzione o manipolazione dei dati.
- Utilizzate gli exploit solo nella misura necessaria a confermare la presenza di una vulnerabilità. Non utilizzate gli exploit per compromettere o sottrarre dati, stabilire un accesso persistente alla riga di comando o passare ad altri sistemi.

L'utente è inoltre tenuto a:

- Rispettare le regole, inclusa la presente politica e qualsiasi altro accordo pertinente. In caso di incongruenze tra la presente politica e qualsiasi altro termine applicabile, prevarranno i termini della presente politica.
- Interagire solo con i propri account di prova.
- Limitare la creazione di account a un massimo di due (2) account per qualsiasi test.
- Utilizzare solo i canali ufficiali per divulgare e/o discutere con noi le informazioni relative alle vulnerabilità.
- Inviare una sola vulnerabilità per segnalazione, a meno che non sia necessario concatenare più vulnerabilità per dimostrarne l'impatto.
- Eliminare in modo sicuro tutti i dati recuperati durante la ricerca una volta inviata la segnalazione.
- Eseguire i test solo sui sistemi inclusi nell'ambito e rispetta i sistemi e le attività che non rientrano nell'ambito.
- Evitare l'uso di strumenti di scansione invasivi o automatizzati ad alta intensità per individuare le vulnerabilità.
- Non divulgare pubblicamente alcuna vulnerabilità senza il previo consenso scritto di Trading.com.
- Non eseguire alcun attacco di tipo "Denial of Service".
- Non eseguire attacchi di ingegneria sociale e/o attacchi alla sicurezza fisica contro gli uffici, gli utenti o i dipendenti di Trading.com.
- Non eseguire test automatizzati/scriptati dei moduli web, in particolare dei moduli "Contattaci" progettati per consentire ai clienti di contattare il nostro team di assistenza clienti.

Una volta stabilita l'esistenza di una vulnerabilità o se si incontrano involontariamente dati sensibili (inclusi informazioni di identificazione personale (PII), informazioni finanziarie o informazioni proprietarie o segreti commerciali di qualsiasi parte), **è necessario interrompere il test, informarci immediatamente e non divulgare questi dati a nessun altro**. È inoltre necessario limitare l'accesso ai dati minimi necessari per dimostrare efficacemente la validità del concetto.

2.3. Segnalazione di una vulnerabilità / Canali ufficiali

Si prega di segnalare eventuali vulnerabilità all'indirizzo vulnerability.disclosure.eu@trading.com, fornendo tutte le informazioni pertinenti. Per accelerare la verifica della segnalazione, si prega di fornire le seguenti informazioni nella comunicazione iniziale:

- Posizione, URL o percorso dell'applicazione in cui è stata rilevata la vulnerabilità.
- Descrizione della vulnerabilità e del potenziale impatto dello sfruttamento.
- Istruzioni per riprodurre la vulnerabilità (possono essere passaggi scritti, un video o una serie di schermate che descrivono in dettaglio la prova di concetto)
- L'indirizzo e-mail, l'user agent e il nome utente (se presente) utilizzati nella piattaforma di trading.
- La tua chiave pubblica PGP per consentire la comunicazione crittografata (se disponibile).

2.4. Ambito

(a) Sistemi/servizi interessati

Domini	www.trading.com/eu/
App Android	App ufficiale trading.com (com.trading.application)

Domini	www.trading.com/eu/
App iOS	App ufficiale trading.com (id1576478434)

(b) Sistemi/servizi esclusi

Qualsiasi servizio (come i servizi connessi), sistema o dominio non espressamente elencato nella sezione "Sistemi/servizi inclusi nell'ambito" sopra riportata è escluso dall'ambito e non è autorizzato per i test. Inoltre, le vulnerabilità riscontrate nei sistemi dei nostri fornitori non rientrano nell'ambito della presente politica e devono essere segnalate direttamente al fornitore in base alla sua politica di divulgazione (se esistente). Se non sei sicuro che un sistema rientri nell'ambito, contattaci all'indirizzo vulnerability.disclosure.eu@trading.com.

(c) Vulnerabilità nell'ambito di applicazione

- Iniezione SQL
- Cross Site Scripting (XSS)
- Esecuzione di codice remoto (RCE)
- Falsificazione delle richieste lato server (SSRF)
- Autenticazione e gestione delle sessioni non funzionanti
- Riferimento diretto non sicuro a oggetti (IDOR)
- Esposizione di dati sensibili
- Traversal di directory/percorso
- Inclusione di file locali/remoti
- Cross Site Request Forgery (CSRF) con impatto dimostrabile elevato
- Reindirizzamento aperto su parametri sensibili
- Acquisizione di sottodomini (per l'acquisizione di sottodomini aggiungere un messaggio cordiale del tipo: "Stiamo lavorando per risolvere il problema e torneremo presto.")

(d) Vulnerabilità fuori dall'ambito

Alcune vulnerabilità sono considerate fuori dall'ambito del Programma di divulgazione delle vulnerabilità. Tali vulnerabilità fuori dall'ambito includono, a titolo esemplificativo ma non esaustivo:

- Problemi di configurazione della posta, incluse le impostazioni SPF, DKIM e DMARC
- Vulnerabilità di clickjacking che non portano ad azioni sensibili, come la modifica dell'account
- Self-XSS (ovvero quando un utente deve essere indotto con l'inganno a incollare codice nel proprio browser web)
- Spoofing dei contenuti con impatto minimo (ad esempio, inserimento di testo non HTML)
- Cross-Site Request Forgery (CSRF) con impatto minimo (ad esempio CSRF nei moduli di accesso o disconnessione)
- Reindirizzamento aperto, a meno che non sia possibile dimostrare un impatto aggiuntivo sulla sicurezza
- Attacchi CRLF in cui l'impatto risultante è minimo
- Iniezione dell'intestazione host con impatto minimo
- Flag *HttpOnly* o *Secure* mancanti su cookie non sensibili
- Mancanza delle best practice nella configurazione SSL/TLS e nei cifrari
- Intestazioni di sicurezza HTTP mancanti o configurate in modo errato (ad es. CSP, HSTS)
- Moduli privi di controlli Captcha
- Enumerazione di nomi utente/e-mail tramite messaggi di errore della pagina di accesso

- Enumerazione di nome utente/e-mail tramite messaggio di errore "Password dimenticata"
- Problemi che richiedono un'interazione improbabile da parte dell'utente
- Complessità della password o qualsiasi altro problema relativo alle politiche relative all'account o alla password
- Mancanza di timeout della sessione
- Attacchi di forza bruta
- Problemi relativi al limite di frequenza per azioni non critiche
- Vulnerabilità di WordPress senza prova di sfruttabilità
- Divulgazione di versioni vulnerabili del software senza prova di vulnerabilità
- Qualsiasi attività che potrebbe causare l'interruzione del nostro servizio (DoS)
- Mancanza di protezione root / Bypass della protezione root (applicazioni mobili)
- Mancanza di pinning del certificato SSL / Bypass del pinning del certificato SSL (applicazioni mobili)
- Mancanza di offuscamento del codice (applicazioni mobili)

2.5. Tempi di risoluzione e risposta

Il team di sicurezza confermerà la ricezione della segnalazione entro tre giorni lavorativi. Collaboreremo con i team interni per verificare la segnalazione e rispondere tempestivamente con un aggiornamento o una richiesta di ulteriori informazioni.

Se la segnalazione inviata viene confermata come valida, il team di sicurezza procederà con la risoluzione o la mitigazione del problema in base all'impatto e alla gravità della segnalazione. Cercheremo di tenervi informati sui nostri progressi durante tutto il processo.

3. RICOMPENSE

Apprezziamo coloro che dedicano tempo e impegno alla segnalazione di vulnerabilità di sicurezza in conformità con la presente politica. Tuttavia, al momento non offriamo alcun premio per la segnalazione di vulnerabilità. Ciò è soggetto a modifiche in futuro.

4. DETTAGLI DELLA CHIAVE PGP

Invitiamo i segnalatori a utilizzare canali di comunicazione crittografati per proteggere la riservatezza delle segnalazioni di vulnerabilità utilizzando la nostra chiave pubblica PGP.

Impronta digitale della chiave PGP: 2F2F9F5449F1F649804F9B7F297F8FD1B8048BCD

Scarica la chiave PGP

Nota: crittografare i messaggi con la chiave PGP sopra indicata e includere la propria chiave pubblica nell'e-mail.

5. FEEDBACK

Se desideri fornire feedback o suggerimenti su questa politica, contattaci all'indirizzo vulnerability.disclosure.eu@trading.com.

Grazie per il tuo contributo alla sicurezza di Trading.com e dei nostri utenti.