trading.com

POLÍTICA DE DIVULGAÇÃO DE VULNERABILIDADES

1. INTRODUÇÃO

Trading.com Markets Inc. (doravante "**Trading.com**") reconhece a necessidade de abordar o comunidade de segurança cibernética para proteger os dados dos clientes e trabalhar em conjunto para criar soluções e aplicativos mais seguros. Esta política tem como objetivo fornecer aos pesquisadores de segurança diretrizes claras para a condução de atividades de descoberta de vulnerabilidades e transmitir nossas preferências sobre como enviar descobriu vulnerabilidades para nós.

Os pesquisadores são bem-vindos a relatar voluntariamente vulnerabilidades que possam encontrar relacionadas ao Sistemas Trading.com. Esta política descreve quais sistemas e tipos de pesquisa estão cobertos por esta política e como enviar para nós relatórios de vulnerabilidade.

A submissão de relatórios de vulnerabilidade está sujeita aos termos e condições estabelecidos neste página e, ao enviar um relatório de vulnerabilidade à Trading.com, os pesquisadores reconhecem que eles leram e concordaram com estes termos e condições.

2. PORTO SEGURO/AUTORIZAÇÃO

Ao conduzir pesquisas de vulnerabilidade, demonstrando esforço de boa-fé para cumprir esta política, consideramos que sua pesquisa é:

- Autorizado, em relação a quaisquer leis anti-hacking aplicáveis e não recomendaremos ou iniciar uma ação legal contra você por sua pesquisa.
- Autorizado em relação a quaisquer leis anti-evasão relevantes e não faremos nenhuma reclamação contra você por contornar os controles de tecnologia.
- Legal, útil para a segurança geral da Internet, e conduzido de boa fé.

Espera-se que você cumpra todas as leis aplicáveis. Se a ação legal for iniciada por terceiros contra você por atividades que você conduziu de boa fé de acordo com esta política, nós dará a conhecer esta autorização.
Se a qualquer momento você tiver preocupações ou são incertos se sua pesquisa de segurança é consistente com esta política, envie um relatório por meio de um de nossos canais oficiais (conforme determinado abaixo) antes de prosseguir.

Observe que o Safe Harbor se aplica apenas a ações judiciais sob o controle da organização participante desta política e que a política não vincula terceiros independentes.

3. DIRETRIZES

De acordo com esta política, "pesquisa" significa atividades nas quais você:

- Notifique-nos o mais rápido possível após descobrir um problema de segurança real ou potencial.
- Faça todos os esforços para evitar violações de privacidade, degradação da experiência do usuário, interrupção do sistemas de produção e destruição ou manipulação de dados.
- Use explorações apenas na medida necessária para confirmar a presença de uma vulnerabilidade. Não use uma exploração para comprometer ou exfiltrar dados, estabelecer acesso persistente à linha de comando, ou usar a exploração para migrar para outros sistemas.

Você também é solicitado a:

- Cumpra as regras, inclusive seguindo esta política e quaisquer outros acordos relevantes. Se houver qualquer inconsistência entre esta política e quaisquer outros termos aplicáveis, os termos de esta política prevalecerá.
- Interaja apenas com suas próprias contas de teste.
- Limite a criação de conta a duas (2) contas no total para qualquer teste.
- Use apenas os Canais Oficiais para divulgar e/ou discutir informações de vulnerabilidade conosco. Envie uma vulnerabilidade por relatório, a menos que você precise encadear vulnerabilidades para demonstrar o impacto.
- Exclua com segurança todos os dados recuperados durante a pesquisa assim que o relatório for enviado.

- Realize testes apenas em sistemas dentro do escopo e respeite sistemas e atividades que estão fora do escopo.
- Evite usar ferramentas de verificação invasivas ou automatizadas de alta intensidade para encontrar vulnerabilidades. Não divulgue publicamente qualquer vulnerabilidade sem o consentimento prévio por escrito da Trading.com. Não execute nenhum procedimento de "Negação de Serviço" ataque.
- Não realize ataques de engenharia social e/ou segurança física contra os sites da Trading.com escritórios, usuários ou funcionários.
- Não execute testes automatizados/com script de formulários da web, especialmente os formulários "Fale Conosco", projetados para que os clientes entrem em contato com nossa equipe de Atendimento ao Cliente.
- Depois de estabelecer que existe uma vulnerabilidade ou encontrar inadvertidamente qualquer dados confidenciais (incluindo informações de identificação pessoal (PII), informações financeiras, ou informações proprietárias ou segredos comerciais de qualquer parte), você deve interromper o teste, notificar-nos imediatamente e não divulgar esses dados a mais ninguém. Você também deve limitar seu acesso a os dados mínimos necessários para demonstrar eficazmente uma prova de conceito.

4. RELATÓRIO DE VULNERABILIDADE/CANAIS OFICIAIS

Por favor, reporte quaisquer vulnerabilidades para vulnerability.disclosure.us@trading.com, fornecendo todas as informações relevantes. Para agilizar a verificação de sua descoberta, forneça as seguintes informações em sua comunicação inicial:

- Localização, URL, ou caminho do aplicativo em que a vulnerabilidade foi descoberta.
- Descrição da vulnerabilidade e do impacto potencial da exploração.
- Instruções para reproduzir a vulnerabilidade (podem ser etapas escritas, um vídeo ou um conjunto de capturas de tela detalhando a prova de conceito).
- O endereço de e-mail, agente do usuário e nome(s) de usuário usados na plataforma de negociação (se houver). Sua chave pública PGP para permitir comunicação criptografada (se disponível).

5. ESCOPO

(a) Sistemas/Serviços no Escopo

Domínio	www.trading.com/us/
Aplicativo Android	aplicativo oficial de negociação.com (com.trading.aplication)
Aplicativo iOS	aplicativo oficial de negociação.com (id1576478434)

(b) Fora de-Sistemas/serviços de escopo

Qualquer serviço (como serviços conectados), sistema ou domínio não listado expressamente no "In-Scope Sistemas/Serviços" seção acima, estão excluídos do escopo e não estão autorizados para testes. Além disso, as vulnerabilidades encontradas em sistemas de nossos fornecedores estão fora do escopo desta política e devem ser relatadas diretamente ao fornecedor de acordo com sua política de divulgação (se houver).. Se você não tem certeza se um sistema está dentro do escopo ou não, entre em contato conosco.

(c) Vulnerabilidades no escopo
- Injeção SQL
- Scripting entre sites (XSS)
- Execução remota de código (RCE)
- Falsificação de solicitação do lado do servidor (SSRF)

- Autenticação quebrada e gerenciamento de sessão
- Referência direta de objeto inseguro (IDOR)
- Exposição de dados confidenciais
- Travessia de diretório/caminho
- Inclusão de arquivos locais/remotos
- Falsificação de solicitação entre sites (CSRF) com alto impacto demonstrável
- Redirecionamento aberto em parâmetros confidenciais
- Aquisição de subdomínio (para aquisição de subdomínio, adicione uma mensagem amigável como: "Estamos trabalhando nisso e voltaremos em breve.")

(d) Fora-Vulnerabilidades fora do escopo

Certas vulnerabilidades são consideradas fora de-escopo do Programa de Divulgação de Vulnerabilidades. Essas vulnerabilidades fora do escopo incluem, mas não estão limitadas a:

- Problemas de configuração de email, incluindo configurações de SPF, DKIM, DMARC
- Vulnerabilidades de clickjacking que não levam a ações confidenciais, como modificação
- Auto-XSS (ou seja, onde um usuário precisaria ser induzido a colar o código em seu navegador)
- Falsificação de conteúdo onde o impacto resultante é mínimo (por exemplo,, injeção de texto não HTML)
- Falsificação de solicitação entre sites (CSRF) onde o impacto resultante é mínimo (por exemplo, CSRF em formulários de login ou logout)
- Redirecionamento aberto - a menos que um impacto adicional na segurança possa ser demonstrado
- Ataques CRLF onde o impacto resultante é mínimo
- Injeção de cabeçalho de host onde o impacto resultante é mínimo Ausente Somente http ou Seguro sinalizadores em cookies não sensíveis
- Faltam práticas recomendadas na configuração e cifras SSL/TLS Cabeçalhos de segurança HTTP ausentes ou configurados incorretamente (por exemplo, CSP, HSTS) Formulários sem controles Captcha
- Enumeração de nome de usuário/e-mail via mensagem de erro da página de login
- Enumeração de nome de usuário/e-mail via mensagem de erro Esqueci a senha
- Problemas que exigem interação improvável do usuário
- Complexidade da senha ou qualquer outro problema relacionado às políticas de conta ou senha
- Falta de tempo limite da sessão
- Bruto-ataques de força
- Problemas de limite de taxa para ações não críticas
- Vulnerabilidades do WordPress sem prova de exploração
- Divulgação de versão de software vulnerável sem prova de exploração
- Qualquer atividade que possa levar à interrupção do nosso serviço (DoS)
- Falta de proteção Root/Ignorar proteção Root (aplicativos móveis)
- Falta de fixação de certificado SSL/Ignorar fixação de certificado SSL (aplicativos móveis)
- Falta de ofuscação de código (aplicativos móveis)

6. TEMPOS DE REMEDIAÇÃO E RESPOSTA

Após a receção do seu relatório, a equipa de segurança confirmará no prazo de três dias úteis. Colaboraremos com as equipas internas para verificar as conclusões e responderemos prontamente com uma atualização ou um pedido de informações adicionais.

Se a constatação apresentada for confirmada como válida, a equipa de segurança avançará com a correção ou atenuação do problema de acordo com o impacto e a gravidade da constatação. Tentaremos mantê-lo informado sobre o nosso progresso ao longo do processo.

7. RECOMPENSAS

Valorizamos aqueles que dedicam tempo e esforço para relatar vulnerabilidades de segurança de acordo com esta política. No entanto, atualmente não oferecemos nenhuma recompensa por divulgação de vulnerabilidades. Isto é assunto mudar no futuro.

8. DETALHES PRINCIPAIS DO PGP

Encorajamos fortemente os repórteres a utilizarem canais de comunicação criptografados, garantindo a confidencialidade dos relatórios de vulnerabilidade usando nossa chave pública PGP.

Impressão digital da chave PGP: 2F2F9F5449F1F649804F9B7F297F8FD1B8048BCD

---INICIAR BLOCO DE CHAVE PÚBLICA PGP ----

MDMEZSUPWXYJKwYBBAHaRw8BAQdAk9xhyMSICuJ8H7DSP6xDeZSaZuEgqXx4HiQka8sYDYOOT1RyYWR
pbmcuY29tIEluZm9ybWF0aW9uIFNIY3VyaXR5IFRIYW0gPHZ1bG5lcmFiaWxpdHkuZGlzY2xvc3VyZS5ldUB0cm
FkaW5nLmNvbT61lgQTFggAPhYhBC8vn1RJ8fZJgE+bfyl/j9G4BlvNBQJIJQ9bAhsDBQKDwmcABQsJCAcCBHU
KCQgLAgQWAgMBAh4BAheAAAoJECI/j9G4BlvNgKMBAOPAFg9sWDt1vKGrUGN1PTZJI2tNCUIBAArUOPs1ag
qpAQD65|XReNFJwVWJGo/NiacLRvfJ5VPOp30M6kv/FbnHArRPVHJhZGluZy5jb20gSW5mb3JtYXRpb24gU2Vj
dXJpdHkgVGVhbSA8dnVsbmVyYWJpbGl0eS5kaXNjbG9zdXJILnVrQHRyYWRpbmcuY29tPoiWBBMWCAA+FIE
ELY+fVEnx9kmAT5t/KX+PObgEi80FAmUID9sCGwMFCQPCZwAFCwkIBwIGFQoJCASCBBYCAWECHgECF4A
ACgkQKX+P0bgEi82Q+gD6AwaAGPgAaXYpf8e+F8pCV/8jWyaHluahPFIn2Lpcu2kBAKpaeCpfKYmr0gVx1UvJG
SwQHstDoxT6IWg7p9pJv4QBtE9UcmFkaW5nLmNvbSBJbmZvcm1hdGlvbiBTZWN1cml0eSBUZWFtIDx2dWxuZ
XJhYmlsaXR5LmRpc2Nsb3N1cmUudXNAdHJhZGluZy5jb20+iJYEEXYAD4WIQQvL59USfH2SYBPm38pf4/RuA
SLzQUCZSUQGWIBAWUJA8JnAAULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRApf4/RuASLZVK9AP9QLAc
QKMIXGTHowMb2WA3y0ayXs0jFDVDF0QSut69GqgEA1TjHkhcm7omdKUFcEb75KyFH6rSj9HjbbvHAdo3Elwu0
T1RyYWRpbmcuY29tIEluZm9ybWF0aW9uIFNIY3VyaXR5IFRIYW0gPHZ1bG5lcmFiaWxpdHkuZGlzY2xvc3VyZS
5hdUB0cmFkaW5nLmNvbT61lgQTFggAPhYhBC8vn1RJ8fZJgE+bfyl/j9G4BIVNBQJIJRATAhsDBQkDwmcABQsJ
CACCBhUKCQgLAgQWAgMBAh4BAheAAAoJECI/j9G4BlvN+2wA/iY8mQlgxReWtiDo9c+YuQx7T+mTNVaucaml
eWBOoeJEAQD/zNdaaB+JUDBWYEZZ4R1YKEA1t/OyTug20jPd11rkCrg4BGUID1sSCisGAQQBI1UBBQEBBOD
fryJ3SKSV3Nx2k9BydwhDd118X/0+08m3QJRgd9WnYwMBCAelfgQYFggAJhYhBC8vn1RJ8fZJgE+bfyl/j9G4BIV
NBQJIJQ9bAhsMBQkDwmcAAAoJECI/j9G4BlvNgacBAJAwuC8SJPDxSqlYdH/m4hA8M1hSZcd/U2Ysrw97HWX
WAP45/yiYXuBjpndmng+KCb1WAHgTMq7rAsCpnoQjrnwm Cw==

=HMGI

----FIM DO BLOCO DE CHAVE PÚBLICA PGP-----

Observação: Solicitamos gentilmente que você criptografe suas mensagens usando a chave PGP fornecida e inclua sua própria chave pública no e-mail.

9. FEEDBACK

Se você deseja fornecer comentários ou sugestões sobre esta política, entre em contato conosco vulnerability.disclosure.us@trading.com.

Obrigado por ajudar a manter a Trading.com e nossos usuários seguros.