trading.com

# POLÍTICA DE DIVULGACIÓN DE VULNERABILIDADES

1. INTRODUCCIÓN

Trading.com Markets Inc. (en adelante "**Trading.com**") reconoce la necesidad de abordar la comunidad de ciberseguridad para proteger los datos de los clientes y trabajar juntos para crear soluciones y aplicaciones más seguras. Esta política tiene como objetivo brindar a los investigadores de seguridad pautas claras para realizar actividades de descubrimiento de vulnerabilidades y transmitir nuestras preferencias sobre cómo enviar nos descubrieron vulnerabilidades.

Los investigadores pueden informar voluntariamente las vulnerabilidades que puedan encontrar relacionadas con el Sistemas Trading.com. Esta política describe **¿Qué sistemas y tipos de investigación?** están cubiertos por esta póliza **y cómo enviar** a nosotros informes de vulnerabilidad.

La presentación de informes de vulnerabilidad está sujeta a los términos y condiciones establecidos en este página, y al enviar un informe de vulnerabilidad a Trading.com, los investigadores reconocen que han leído y aceptado estos términos y condiciones.

2. PUERTO SEGURO/AUTORIZACIÓN

Al realizar una investigación de vulnerabilidad, mostrando un esfuerzo de buena fe para cumplir con esta política, consideramos que su investigación es:

- Autorizado, en relación con las leyes anti-piratería aplicables y no recomendaremos ni emprender acciones legales en su contra por su investigación.
- Autorizado en relación con cualquier ley antielusión relevante y no presentaremos un reclamo contra usted por elusión de controles tecnológicos..
- Legal, útil para la seguridad general de Internet, y realizado de buena fe.

Se espera que usted cumpla con todas las leyes aplicables.. Si la acción legal es iniciada por un tercero contra usted por actividades que haya realizado de buena fe de acuerdo con esta política, dará a conocer esta autorización.

Si en algún momento tienes dudas o están inseguros Si su investigación de seguridad es consistente con esta política, envíe un informe a través de uno de nuestros canales oficiales (como se determina a continuación) antes de continuar..

Tenga en cuenta que Safe Harbor se aplica únicamente a reclamaciones legales bajo el control de la organización que participa en esta política, y que la política no vincula a terceros independientes.

3. DIRECTRICES

Según esta política, "investigación" significa actividades en las que usted:

- Notifíquenos lo antes posible después de descubrir un problema de seguridad real o potencial.
- Haga todo lo posible para evitar violaciones de la privacidad, degradación de la experiencia del usuario, interrupción de sistemas de producción, y destrucción o manipulación de datos.
- Utilice exploits únicamente en la medida necesaria para confirmar la presencia de una vulnerabilidad. no usar un exploit para comprometer o filtrar datos, establecer un acceso persistente a la línea de comandos, o utilizar el exploit para pasar a otros sistemas.

También se le solicita:

- Respete las reglas, incluido el cumplimiento de esta política y cualquier otro acuerdo relevante. Si hay alguna inconsistencia entre esta política y cualquier otro término aplicable, los términos de esta política prevalecerá.
- Interactúa solo con tus propias cuentas de prueba.

- Limite la creación de cuentas a dos (2) cuentas en total para cualquier prueba.
- Utilice únicamente los canales oficiales para revelar y/o discutir información sobre vulnerabilidades con nosotros..
- Envíe una vulnerabilidad por informe, a menos que necesite encadenar vulnerabilidades para demostrar el impacto.
- Elimine de forma segura todos los datos recuperados durante la investigación una vez que se envíe el informe.
- Realice pruebas solo en sistemas dentro del alcance y respete los sistemas y actividades que estén fuera del alcance.
- Evite el uso de herramientas de escaneo automatizadas o invasivas de alta intensidad para encontrar vulnerabilidades..
- No revele públicamente ninguna vulnerabilidad sin el consentimiento previo por escrito de Trading.com..
- No realice ninguna "Denegación de Servicio" ataque.
- No realice ataques de ingeniería social y/o de seguridad física contra los sitios web de Trading.com. oficinas, usuarios o empleados.
- No realice pruebas automatizadas/programadas de formularios web, especialmente los formularios "Contáctenos" que están diseñados para que los clientes se comuniquen con nuestro equipo de Atención al Cliente.
- Una vez que haya establecido que existe una vulnerabilidad o que encuentre involuntariamente alguna datos confidenciales (incluida la información de identificación personal (PII), información financiera, o información de propiedad exclusiva o secretos comerciales de cualquier parte), debe detener la prueba, notificarnos inmediatamente y no revelar estos datos a nadie más. También debe limitar su acceso a los datos mínimos necesarios para demostrar eficazmente una prueba de concepto.

4. REPORTAR VULNERABILIDAD/CANALES OFICIALES

Por favor informe cualquier vulnerabilidad a vulnerability.disclosure.us@trading.com, proporcionando toda la información relevante. Para acelerar la verificación de su hallazgo, Por favor proporcione la siguiente información en su comunicación inicial.:

- Ubicación, URL, o ruta de la aplicación donde se descubrió la vulnerabilidad.
- Descripción de la vulnerabilidad y el impacto potencial de la explotación.
- Instrucciones para reproducir la vulnerabilidad (pueden ser pasos escritos, un vídeo o un conjunto de capturas de pantalla que detallan la prueba de concepto).
- La dirección de correo electrónico, el agente de usuario y los nombres de usuario utilizados en la plataforma de negociación (si corresponde).
- Su clave pública PGP permite la comunicación cifrada (si está disponible).

5. ALCANCE

(a) Sistemas/Servicios dentro del alcance

| | |
|---|---|
| Dominio | www.trading.com/us/ |
| Aplicación de Android | aplicación oficial de trading.com (com.trading.aplication) |
| Aplicación para iOS | aplicación oficial de trading.com (id1576478434) |

(b) Fuera de-Sistemas/Servicios de Alcance

Cualquier servicio (como servicios conectados), sistema o dominio que no figura expresamente en el "Alcance Sistemas/Servicios" sección anterior, están excluidos del alcance y no están autorizados para realizar pruebas. Además, las vulnerabilidades encontradas en los sistemas de nuestros proveedores quedan fuera del alcance de esta política y deben informarse directamente al proveedor de acuerdo con su política de divulgación (si corresponde).. Si no está seguro de si un sistema está dentro del alcance o no, contáctenos.

(c) Vulnerabilidades dentro del alcance

- Inyección SQL
- Secuencias de comandos entre sitios (XSS)
- Ejecución remota de código (RCE)
- Falsificación de solicitudes del lado del servidor (SSRF)
- Autenticación rota y gestión de sesiones
- Referencia directa a objetos inseguros (IDOR)
- Exposición de datos confidenciales
- Recorrido de directorio/ruta
- Inclusión de archivos locales/remotos
- Falsificación de solicitudes entre sitios (CSRF) con alto impacto demostrable
- Abrir redirección en parámetros sensibles
- Adquisición de subdominio (para la adquisición de subdominio, agregue un mensaje amigable como: "Estamos trabajando en ello y volveremos pronto.")

(d) Fuera-Vulnerabilidades fuera de alcance

Ciertas vulnerabilidades se consideran fuera de-alcance del Programa de Divulgación de Vulnerabilidades. Esas vulnerabilidades fuera de alcance incluyen, entre otras:

- Problemas de configuración de correo, incluidas las configuraciones SPF, DKIM y DMARC
- Vulnerabilidades de clickjacking que no conducen a acciones confidenciales, como la cuenta modificación
- Self-XSS (es decir, donde sería necesario engañar a un usuario para que pegue el código en su navegador web)
- Suplantación de contenido cuando el impacto resultante es mínimo (p. ej., inyección de texto no HTML)
- Falsificación de solicitudes entre sitios (CSRF) donde el impacto resultante es mínimo (por ejemplo, CSRF en formularios de inicio o cierre de sesión)
- Redirección abierta: a menos que se pueda demostrar un impacto adicional en la seguridad
- Ataques CRLF donde el impacto resultante es mínimo
- Inyección del encabezado del host donde el impacto resultante es mínimo. Falta Sólo Http o Seguro banderas en cookies no sensibles
- Faltan mejores prácticas en configuración y cifrados SSL/TLS Encabezados de seguridad HTTP faltantes o mal configurados (por ejemplo, CSP, HSTS)
- Faltan controles Captcha en los formularios
- Enumeración de nombre de usuario/correo electrónico a través del mensaje de error de la página de inicio de sesión
- Enumeración de nombre de usuario/correo electrónico a través del mensaje de error Olvidé mi contraseña
- Problemas que requieren una interacción poco probable del usuario
- Complejidad de la contraseña o cualquier otro problema relacionado con las políticas de cuenta o contraseña
- Falta de tiempo de espera de la sesión
- Bruto-ataques de fuerza
- Problemas de límite de velocidad para acciones no críticas

- Vulnerabilidades de WordPress sin prueba de explotabilidad
- Divulgación de versión de software vulnerable sin prueba de explotabilidad
- Cualquier actividad que pueda provocar la interrupción de nuestro servicio (DoS)
- Falta de protección Root / Omisión de protección Root (aplicaciones móviles)
- Falta de fijación de certificados SSL/Omisión de fijación de certificados SSL (aplicaciones móviles)
- Falta de ofuscación de código (aplicaciones móviles)

6. TIEMPOS DE REMEDIACIÓN Y RESPUESTA

Una vez recibido su informe, el equipo de Seguridad lo confirmará en un plazo de tres días laborables. Colaboraremos con los equipos internos para verificar los hallazgos y responderemos rápidamente con una actualización o solicitud de información adicional.

Si se confirma que el hallazgo presentado es válido, el equipo de seguridad procederá a poner remedio o mitigar el problema en función del impacto y la gravedad del hallazgo. Intentaremos mantenerte informado de nuestros progresos a lo largo del proceso.

7. RECOMPENSAS

Valoramos a quienes se toman el tiempo y el esfuerzo de informar vulnerabilidades de seguridad de acuerdo con esta política. Sin embargo, actualmente no ofrecemos ninguna recompensa por la divulgación de vulnerabilidades. Este es el tema para cambiar en el futuro.

8. DETALLES DE LA CLAVE PGP

Recomendamos encarecidamente a los periodistas que utilicen canales de comunicación cifrados, garantizando la confidencialidad de los informes de vulnerabilidad utilizando nuestra clave pública PGP.

**huella digital de clave PGP:** 2F2F9F5449F1F649804F9B7F297F8FD1B8048BCD

---- COMENZAR BLOQUE DE LLAVE PÚBLICA PGP----

MDMEZSUPWXYJKwYBBAHaRw8BAQdAk9xhyMSICuJ8H7DSP6xDeZSaZuEgqXx4HiQka8sYDYOOT1
RyYWRpbmcuY29tIEluZm9ybWF0aW9uIFNIY3VyaXR5IFRIYW0gPHZ1bG5lcmFiaWxpdHkuZGlzY2xvc3
VyZS5ldUB0cmFkaW5nLmNvbT61lgQTFggAPhYhBC8vn1RJ8fZJgE+bfyl/j9G4BlvNBQJIJQ9bAhsDBQK
DwmcABQsJCAcCBHUKCQgLAgQWAgMBAh4BAheAAAoJECI/j9G4BlvNgKMBAOPAFg9sWDt1vKGrU
GN1PTZJI2tNCUIBAArUOPs1agqpAQD65|XReNFJwVWJGo/NiacLRvfJ5VPOp30M6kv/FbnHArRPVHJh
ZGluZy5jb20gSW5mb3JtYXRpb24gU2VjdXJpdHkgVGVhbSA8dnVsbmVyYWJpbGl0eS5kaXNjbG9zdXJl
LnVrQHRyYWRpbmcuY29tPoiWBBMWCAA+FIEELY+fVEnx9kmAT5t/KX+PObgEi80FAmUID9sCGwMF
CQPCZwAFCwkIBwIGFQoJCASCBBYCAWECHgECF4AACgkQKX+P0bgEi82Q+gD6AwaAGPgAaXYpf
8e+F8pCV/8jWyaHluahPFln2Lpcu2kBAKpaeCpfKYmr0gVx1UvJGSwQHstDoxT6lWg7p9pJv4QBtE9Ucm
FkaW5nLmNvbSBJbmZvcm1hdGlvbiBTZWN1cml0eSBUZWFtIDx2dWxuZXJhYmlsaXR5LmRpc2Nsb3N1
cmUudXNAdHJhZGluZy5jb20+iJYEEXYAD4WIQQvL59USfH2SYBPm38pf4/RuASLzQUCZSUQGWIBA
WUJA8JnAAULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRApf4/RuASLZVK9AP9QLAcQKMIXGTHow
Mb2WA3y0ayXs0jFDVDF0QSut69GqgEA1TjHkhcm7omdKUFcEb75KyFH6rSj9HjbbvHAdo3Elwu0T1RyY
WRpbmcuY29tIEluZm9ybWF0aW9uIFNIY3VyaXR5IFRIYW0gPHZ1bG5lcmFiaWxpdHkuZGlzY2xvc3VyZ
S5hdUB0cmFkaW5nLmNvbT61lgQTFggAPhYhBC8vn1RJ8fZJgE+bfyl/j9G4BIVNBQJIJRATAhsDBQkDw
mcABQsJCACCBhUKCQgLAgQWAgMBAh4BAheAAAoJECI/j9G4BlvN+2wA/iY8mQlgxReWtiDo9c+YuQ
x7T+mTNVaucamleWBOoeJEAQD/zNdaaB+JUDBWYEZZ4R1YKEA1t/OyTug20jPd11rkCrg4BGUID1sS
CisGAQQBI1UBBQEBBODfryJ3SKSV3Nx2k9BydwhDd118X/0+08m3QJRgd9WnYwMBCAelfgQYFggAJ
hYhBC8vn1RJ8fZJgE+bfyl/j9G4BIVNBQJIJQ9bAhsMBQkDwmcAAAoJECI/j9G4BlvNgacBAJAwuC8SJP
DxSqlYdH/m4hA8M1hSZcd/U2Ysrw97HWXWAP45/yiYXuBjpndmng+KCb1WAHgTMq7rAsCpnoQjrnwm
Cw==

=HMGI
-FIN BLOQUE DE LLAVE PÚBLICA PGP-----

**Nota**: Le solicitamos amablemente que cifre sus mensajes utilizando la clave PGP proporcionada e incluya su propia clave pública en el correo electrónico.

9. COMENTARIOS

Si desea enviar comentarios o sugerencias sobre esta política, comuníquese con nosotros at vulnerability.disclosure.us@trading.com.

Gracias por ayudar a mantener Trading.com y a nuestros usuarios seguros.