Comunicación de vulnerabilidad

Nota: las vulnerabilidades se deben informar de forma **individual** según el modelo establecido. El equipo de Seguridad de VTEX no atenderá vulnerabilidades que no sigan el patrón establecido. Si encontraste más de una vulnerabilidad en tu prueba, rellena varios modelos y adjúntalos a tu ticket.

Información sobre la vulnerabilidad:

1. Título/Resumen
2. Nombre de la cuenta VTEX
3. Número CVE de referencia de la vulnerabilidad, si hay
4. Descripción completa del descubrimiento
    a. Cómo se detectó la vulnerabilidad
    b. Pruebas
5. Las URL y flujos afectados
6. Pasos necesarios para reproducir o identificar la vulnerabilidad
7. Posibles problemas causados por la vulnerabilidad
8. Recomendación de corrección
9. Gravedad (**según el framework CVSS 3.1**)
    a. Crítica
    b. Alta
    c. Media
    d. Baja
10. Metodología utilizada
11. Adjuntos y pruebas