



Divulgação de Vulnerabilidade Ética

A VTEX possui um canal para receber comunicações sobre potenciais vulnerabilidades em seus sistemas e se compromete a não “processar” os usuários que os reportam, desde que as regras abaixo sejam cumpridas:

1. Apenas sistemas da VTEX são testados. Nós não autorizamos o teste em páginas de clientes ou fornecedores.
2. As páginas disponíveis para testes são:
 - a. Use securitystore.myvtex.com (e outros e.g.) como ponto de entrada
 - b. Domínios em escopo são as propriedades da VTEX utilizadas para suportar a loja:
 - c. vtexassetsj
 - d. vtex.io
 - e. vtexcommercesable
 - f. vtexpayments
3. O pesquisador de segurança realizando o teste deve:
 - a. criar contas próprias de usuário;
 - b. evitar violações da privacidade de outras pessoas, incluindo outros pesquisadores de segurança;
 - c. reportar falhas assim que as encontrar, e não usar falhas para “escalar” acesso;
 - d. fazer um esforço de boa-fé para evitar danos ao ambiente de produção da VTEX (e.g. não tentar deleções em massa, ataques de DoS, etc. etc.);
 - e. dar à VTEX um tempo razoável para investigar e solucionar problemas de segurança antes de publicar o resultado das iterações;
4. A VTEX se reserva o direito de:
 - a. distribuir o conteúdo dos reports internamente e compartilhá-los com quaisquer terceiros que achar necessário;
 - b. publicar interações com os pesquisadores (incluindo programas);
 - c. agradecer publicamente os pesquisadores que reportaram falhas;
 - d. investigar qualquer atividade que possa ser atribuída à pessoa enviando o report em outras;
 - e. executar qualquer programa enviado como PoC;
 - f. mudar as regras deste programa;

Você pode entrar em contato por security AT vtex.com

