Política de Divulgação Coordenada de Vulnerabilidades Seventh

A Seventh, empresa que oferece soluções inovadoras em sistemas de segurança eletrônica, está empenhada em garantir a proteção de nossos clientes e usuários, promovendo uma parceria aberta com a comunidade de segurança. Para isso, estamos formalizando a presente política para receber relatórios de vulnerabilidade em seus produtos.

A Política de Divulgação Coordenada de Vulnerabilidades fornece diretrizes para que pesquisadores de segurança descubram e relatem, de forma responsável, as vulnerabilidades em potencial identificadas nos produtos Seventh.

ESCOPO INICIAL

O processo de Divulgação Coordenada de Vulnerabilidades da Seventh abrange os seguintes produtos em nuvem:

- Situator Cloud;
- D-Guard Cloud;
- Portaria Na Nuvem;
- Condomínio Autônomo;
- Controle de Acesso Autônomo; e
- Porteria en la Nube.

Os pesquisadores que nos enviarem um relatório de vulnerabilidade que estiverem dentro dos critérios e forem de interesse da Seventh, receberão crédito sobre a autoria do descobrimento da vulnerabilidade, uma vez que o envio foi aceito e validado por nossa equipe de segurança do produto.

REGRAS, CRITÉRIOS DE ACEITE E PRIORIZAÇÃO

A vulnerabilidade relatada pelo pesquisador estará sujeita à análise da Seventh, onde serão definidos critérios e priorização das submissões, conforme abaixo:

- O relatório deve ser bem redigido em português ou inglês;
- O relatório deve conter provas de conceito para facilitar a validação e a triagem, bem como, deve ser mencionado o bug, o impacto, e alguma potencial remediação;
- A vulnerabilidade relatada deve estar dentro do escopo dos produtos acima mencionado, caso contrário, terão prioridade baixa na análise da Seventh;
- Relatórios apenas com telas de erro ou saída de ferramentas automatizadas terão prioridade baixa;
- Devem ser mencionados os planos e intenções para a divulgação pública;

- O reporte de vulnerabilidade não pode ser realizado por um colaborador do Grupo Seventh, ou por quem tenha trabalhado na empresa nos últimos 12 (doze) meses;

- O pesquisador deve utilizar com cautela serviços que possam impactar os usuários, bem como, se compromete a não utilizar indevidamente nenhum dado pessoal ou sensível identificado nos produtos;

O QUE VOCÊ PODE ESPERAR DE NÓS:

- Uma resposta oportuna ao seu e-mail (dentro de 5 dias úteis);

- Após a triagem, lhe enviaremos um prazo de correção esperado e seremos transparentes em casos que o produto enfrente desafios para ser corrigido;

- Diálogo aberto para discutir questões relacionadas à vulnerabilidade;

- Notificação de quando a vulnerabilidade foi confirmada por nossa equipe de segurança;

- Créditos sobre a descoberta da vulnerabilidade após sua validação e correção.

POSTURA LEGAL

A Seventh não tem intenção de se envolver em discussões legais contra indivíduos que enviarem relatórios de vulnerabilidade através do nosso Grupo de Resposta a Incidente de Segurança, desde que os relatórios cumpram os requisitos e critérios estabelecidos nessa política, e englobem os itens abaixo:

- Envolvam-se em testes de sistemas ou produtos sem prejudicar a Seventh e/ou seus clientes;

- Participem de testes de vulnerabilidade dentro do escopo de nossa Política de Divulgação de Vulnerabilidades.

- Recebam permissão e consentimento do cliente antes de se envolver em testes de vulnerabilidade contra seus produtos, sistemas etc.;

- Estejam de acordo com as leis brasileiras e do país onde o pesquisador estiver realizando a pesquisa; sua geolocalização;

- Abstenham-se de divulgar detalhes da vulnerabilidade ao público antes de 90 dias corridos ou até que um prazo mutuamente acordado expire;

A participação no processo de Divulgação Coordenada de Vulnerabilidades Seventh não concede nenhum direito de propriedade intelectual ou direito de propriedade sobre os produtos e serviços da Seventh aos pesquisadores participantes ou a qualquer outro terceiro.

Os direitos sobre a propriedade intelectual são de titularidade exclusiva da Seventh ou de seus parceiros, e por conta disso, não podem ser copiados, reproduzidos, transmitidos, exibidos, vendidos, licenciados ou, ainda, explorados para qualquer outra finalidade.

COMO RELATAR UMA VULNERABILIDADE

Para comunicar uma vulnerabilidade em um dos produtos Seventh, por favor, preencha o **formulário de vulnerabilidades** na página da Equipe de

Resposta e Tratamento de Incidentes de Segurança da Informação da Seventh (GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA - **https://novidades.seventh.com.br/vulnerabilidades**).

Ao relatar uma vulnerabilidade, o pesquisador confirma que compreende e aceita a política e os termos e condições.