POLÍTICA DE DIVULGAÇÃO DE VULNERABILIDADES TECH2MOVE

A Tech2Move é uma empresa comprometida em oferecer soluções inovadoras em segurança, redes, comunicação e energia, sempre zelando pela proteção e segurança dos nossos clientes. Formalizamos esta política para receber relatórios de vulnerabilidade em nossos produtos, promovendo uma parceria aberta com a comunidade de segurança com o objetivo de reforçar a confiança e a proteção de nossos usuários.

A Política de Divulgação Coordenada de Vulnerabilidades oferece diretrizes para que pesquisadores de segurança possam identificar e relatar, de maneira responsável, vulnerabilidades em potencial nos produtos Tech2Move.

SOBRE ATUALIZAÇÕES DE FIRMWARE

A atualização do firmware é essencial para um desempenho ideal em cada dispositivo. É muito importante instalar atualizações quando elas são lançadas. Quando a Wavlink lança uma atualização de firmware, eles geralmente contêm melhorias, como novos recursos ou corrigem um bug que pode causar uma vulnerabilidade de segurança ou um problema de desempenho.

Esse processo também é necessário se você encontrar o seguinte:

- Desconexão de rede frequente ou conexão intermitente usando o dispositivo
- Conexão lenta

Uma atualização de firmware pode eliminar esses problemas e ajudar a manter a sua rede segura.

REGRAS, CRITÉRIOS DE ACEITE E PRIORIZAÇÃO

As vulnerabilidades relatadas serão analisadas pela Tech2Move, onde serão estabelecidos critérios e prioridades com base nas seguintes diretrizes:

- As vulnerabilidades devem ser relatadas através do canal de comunicação dedicado. A Tech2Move pode receber relatórios de outros canais, mas não garante que o relatório será reconhecido.

- O relatório deve ser claro e bem redigido em português ou inglês;

- Deve incluir provas de conceito, com uma descrição detalhada do bug, impacto e sugestões de solução;

- A vulnerabilidade relatada deve estar dentro do escopo dos produtos mencionados e devem ser baseados na firmware mais recente lançada, caso contrário, terá prioridade baixa;

- Relatórios que contenham apenas capturas de tela ou saídas de ferramentas automatizadas terão prioridade baixa;

- Devem ser incluídos os planos e intenções para a divulgação pública da vulnerabilidade;

- O pesquisador compromete-se a não utilizar dados pessoais ou sensíveis dos produtos, é necessário aderir aos princípios de proteção de dados o tempo todo e não violar a privacidade e a segurança de

dados dos usuários, funcionários, agentes, serviços ou sistemas da Tech2Move durante o processo de descoberta de vulnerabilidades.

- A Tech2Move não está operando atualmente um programa de recompensa por vulnerabilidades.

COMO A TECH2MOVE LIDARÁ COM VULNERABILIDADES

- Uma resposta aos relatórios de vulnerabilidade o mais rápido possível, geralmente dentro de cinco dias úteis;

- Após a triagem, um prazo estimado de correção será informado e, em caso de desafios, seremos transparentes, podemos entrar em contato se precisarmos de mais informações sobre a vulnerabilidade relatada;

- A remediação geralmente leva até 90 dias e, em alguns casos, pode levar mais tempo;

- Você pode se manter atualizado sobre nosso progresso e a conclusão de quaisquer atividades de remediação.

- A participação no processo de Divulgação de Vulnerabilidades não confere ao pesquisador quaisquer direitos de propriedade intelectual sobre os produtos ou serviços Tech2Move. Todos os direitos de propriedade intelectual permanecem sob a titularidade exclusiva da Tech2Move e de seus parceiros.

COMO RELATAR UMA VULNERABILIDADE

Para comunicar uma vulnerabilidade em um produto Tech2Move, preencha o formulário de vulnerabilidades disponível na página https://suporte.tech2move.com.br/seguranca

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