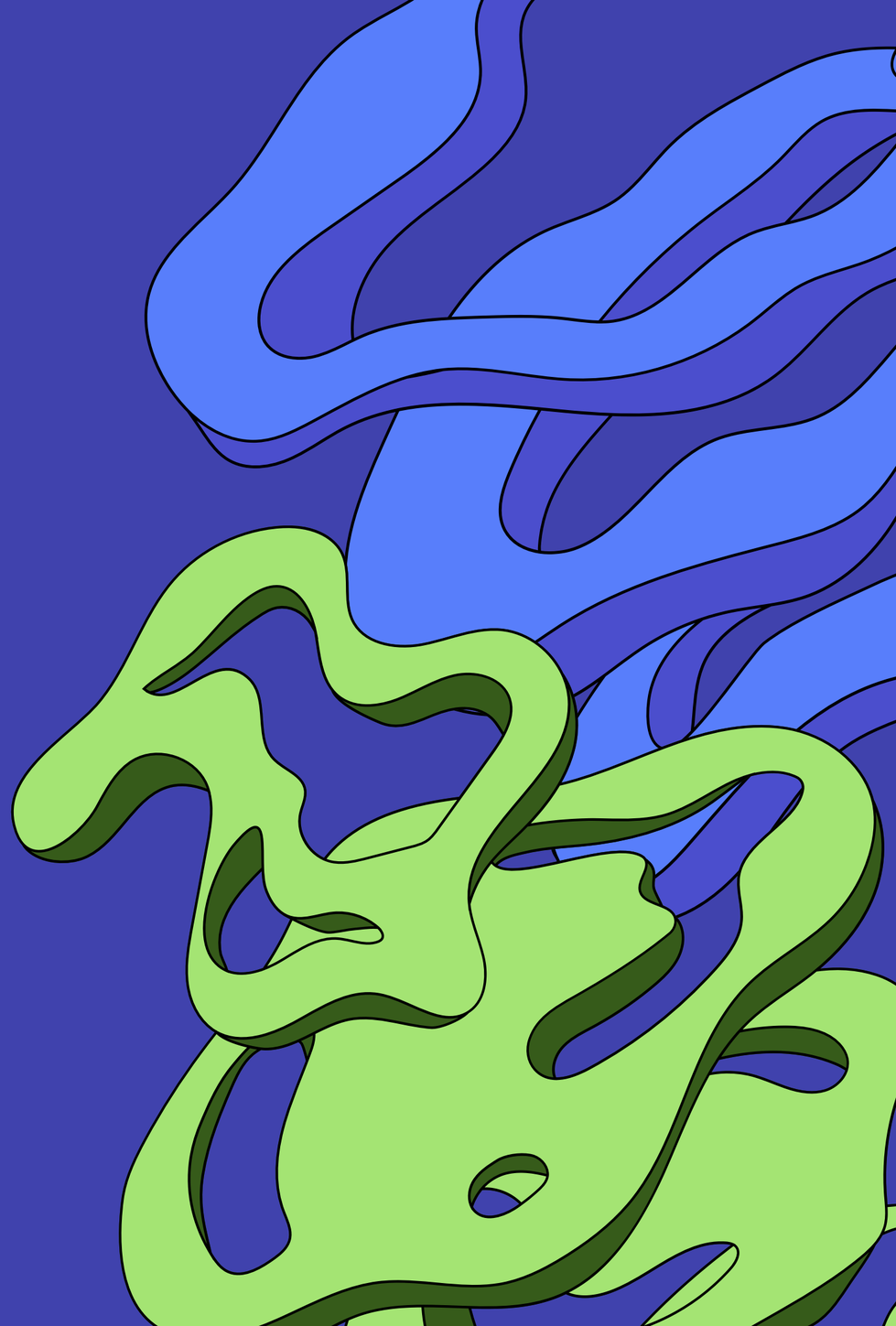
SmarTopia

Análise de segurança do projetp



Brute Force Attack

- **O que é?**

Um ataque de força bruta é uma técnica em que um invasor tenta todas as possíveis combinações de caracteres para descobrir senhas, credenciais e chaves privadas.

- **Como pode ocorrer no projeto?**

Para utilizar os serviços nos clusters em núvem (HIVEMQ, MongoDB e Kafka), deve-se realizar autenticação para acessá-los. Um ataque de Brute Force poderia mirar em descobrir essas credenciais a fim de desabilitar recursos e prejudicar a performance da solução.

- **Mitigação**

Uso de algoritmos de criptografia robustos, geração de chaves longas e aleatórias, evitar engenharia social.

Distributed Denial of Service (DDoS)

- **O que é?**

Utilização de uma botnet (Rede de bots controlados por um atacante) para criar um fluxo excessivo de requisições maliciosas que paralisa um serviço, tornando-o inacessível para usuários legítimos .

- **Como pode ocorrer no projeto?**

Um grande número de mensagens e solicitações de conexão podem sobrecarregar o broker. Sensores e dispositivos IoT podem ser suscetíveis a malwares de forma a serem configurados para enviar mensagens e consumir rapidamente os recursos do broker.

- **Mitigação**

Autenticação e autorização nos servidores MQTT, implementação de firewalls e sistemas de detecção de intrusão, atualização de firmware dos dispositivos IoT.

Man in the middle

- **O que é?**

Tal ataque ocorre quando a comunicação entre duas partes é interceptada por um terceiro. Neste contexto, o invasor pode consumir o conteúdo em trânsito, modificá-lo e eventualmente se passar por uma das partes envolvidas e obtendo acesso não autorizado à informações sensíveis.

- **Como pode ocorrer no projeto?**

No contexto específico de MQTT, esse ataque pode ocorrer na fase de handshake, onde o cliente e o broker estão estabelecendo a conexão ou durante a troca de mensagens.

- **Mitigação**

Uso de criptografia TLS/SSL, autenticação mútua e uso de firewalls.

NoSQL Injection

- **O que é?**

NoSQL Injection é quando um invasor explora vulnerabilidades de segurança no sistema de banco de dados não relacional para manipular consultas ou comandos de forma maliciosa, semelhante ao SQL Injection em bancos de dados relacionais. Esses ataques visam explorar a falta de validação ou sanitização de entradas de dados para executar operações não autorizadas.

- **Como pode ocorrer no projeto?**

Apesar de existir uma forma muito restrita de inserir os dados no MongoDB, utilizando drivers próprios que reforçam a segurança, payloads maliciosos podem ser injetados no banco de forma a comprometer a qualidade dos dados e consequentemente das informações.

- **Mitigação**

Práticas de segurança, como validação de entrada de dados, uso de parâmetros seguros em consultas e controle de acesso adequado ao banco de dados MongoDB.

Conclusão

Devido à natureza não sensível e objetiva dos dados do projeto, ligados à coleta de informações ambientais e sua divulgação pública, os possíveis impactos adversos são considerados moderados e podem ser gerenciados de forma proativa com recursos limitados.

No entanto, é fundamental reconhecer que ataques direcionados à disponibilidade do sistema e à integridade dos dados, especialmente relacionados ao funcionamento dos serviços em nuvem e à qualidade dos dados, podem acarretar consequências mais graves. Portanto, é crucial priorizar a implementação das medidas de mitigação propostas anteriormente, devido à urgência em fortalecer as defesas contra tais ameaças.