**the list of systems of company:**

- transportation system (eg GPS management software)

- Customer information management system, shipping orders (usually using websites)

**the operational characteristics:**

* Transportation system:

**- Vehicle monitoring and tracking:** Provides the ability to monitor the location of transport vehicles in real time.

**- Scheduling and route optimization:** Optimize routes to reduce operating costs and transit times.

**- Alerts and notifications:** Send alerts about incidents such as traffic jams, vehicles stopping unexpectedly, or going off the expected route.

* Customer information management system:

**- Order management:** Monitor the status and processing progress of orders from placing to delivery.

**- Customer management:** Store and manage customer information, including transaction history and service requests.

**- Customer communication:** Provides communication tools between customers and service providers, such as email, chat, and calling.

**hardware & software assets**

* Transportation system:

**- GPS devices**: Include GPS devices mounted on vehicles to collect location data.

**- Server and network system:** Server to process and store data, network system to transmit information.

**- Management software:** Specialized software to monitor, analyze and manage data from GPS devices.

* Customer information management system:

**- Web server:** Server system to store and operate the website to manage orders and customer information.

**- Management software:** CRM (Customer Relationship Management) software and ERP (Enterprise Resource Planning) systems to manage operational processes.

**- Information security:** Firewall system, data encryption, and other security measures to protect customer and order data.

**data and information assets:**

* Transportation system:

**- Location data:** Information about the real-time location of vehicles.

**- Journey history:** Stored data about routes traveled, travel time and stops.

* Customer information management system:

**- Customer data:** Personal information, transaction history, and customer contact information.

**- Order data:** Details about orders, processing status, and other related information.

**- Shipping data:** Information about delivery schedules, shipping service providers, and related information.

**facilities & supplies:**

**- Network infrastructure:** Ensure stable and secure internet connection for online data access and management.

**- Storage devices:** Data storage devices such as hard drives, cloud - storage systems, and data backup measures.

**technical vulnerabity:**

* Transportation system:

CVE-2020-29389:

**- Description:** A vulnerability in the SinoTrack ST-901 GPS Tracker system allows attackers to perform SQL Injection via SMS parameters.

**- Impact:** An attacker can access the GPS device's database, modify or delete data.

**- Solution:** Update the firmware from the manufacturer or apply security measures such as input filtering.

* Customer information management system:

CVE-2019-12314:

**- Description:** Vulnerability in Apache Struts allows attackers to remotely execute code via unauthenticated requests.

**- Impact:** Impacts web applications using Apache Struts, including order management systems and customer information.

**- Solution:** Update to the latest version of Apache Struts that fixes this vulnerability.

**administrative controls:**

**1: Information security policy:**

**- Description:** Establish and implement information security policy including regulations on password management, access rights, data encryption and security incident handling.

**- Minimized risks:**

**+ Threats:** Unauthorized access, information leaks, remote attacks.

**+ Vulnerability:** Inappropriate access rights, weak authentication.

**2: Security training for employees:**

**- Description:** Organize regular training courses on security awareness, including how to identify and prevent attacks such as phishing and social engineering.

**- Minimized risks:**

**+ Threat:** Phishing attacks, information theft via social engineering.

**+ Vulnerability:** Poor security awareness of employees.

**physical controls:**

**1: Physical access control:**

**- Description :** Use an access control system with magnetic cards, fingerprints or facial recognition to limit access to important areas such as data centers and server rooms.

**- Minimized risks :**

**+ Threat :** Unauthorized access to critical infrastructure.

**+ Vulnerability :** The data storage area is not properly protected.

**2: Security monitoring and warning:**

**- Description :** Install surveillance camera systems and security warning sensors in important areas to detect and quickly respond to physical security incidents.

**- Minimized risks :**

**+ Threats :** Illegal intrusion, property destruction.

**+ Vulnerability :** Lack of ability to monitor and respond promptly to physical problems.