CVSS Scoring for Vulnerabilities in Robotic Systems

Scenario Description:

A robotic arm is being used in an automated manufacturing line. The robot is connected to a local network for remote diagnostics, updates, and system monitoring. However, the robot has a vulnerability in its web interface, which allows for unauthenticated access to sensitive configuration settings (e.g., robot arm position, speed, and motion commands). An attacker can exploit this vulnerability to take control of the robot and cause significant damage to production or even disrupt the entire manufacturing line.

The vulnerability is being evaluated for the following potential impacts:

Confidentiality: The vulnerability could allow unauthorized access to sensitive business data, such as order processing information and customer details.

Integrity: An attacker could alter the robot's movements, leading to incorrect handling of inventory or damaging goods.

Availability: The robot could be rendered inoperable, disrupting the entire warehouse operation, which could delay shipments and affect the company's ability to fulfill orders.

Exercise Instructions:

Assess the Base Score

You will calculate the CVSS Base Score for the vulnerability discovered in the robotic system using the metrics mentioned below. You can use the CVSS v3.1 calculator available online.

Use the following CVSS v3.1 metrics for your calculation:

Attack Vector (AV): How is vulnerability accessed?

Attack Complexity (AC): Is the attack easy or difficult to execute?

Privileges Required (PR): Does the attacker need special access rights to exploit vulnerability?

User Interaction (UI): Does the attack require the user to perform any actions?

Confidentiality Impact (C): What is the impact on confidentiality if the vulnerability is exploited?

Integrity Impact (I): What is the impact on the integrity of the system?

Availability Impact (A): What is the impact on the system's availability?