Threat Prioritization List

1) CVE-2023-6943: An attacker may be able to execute a malicious code by remotely calling a function with a path to a malicious library while connected to the products. As a result, unauthorized users may disclose, tamper with, destroy or delete information in the products, or cause a denial-of-service (DoS) condition on the products. This is a much more critical risk for a factory.

2) CVE-2024-21917: This vulnerability allows easy access and hacking of other ftsp systems if one ftsp system on the network is hacked. It makes it easier for an attacker to take over other systems within a factory, which is why it is ranked in this order.

3) CVE-2023-6942: A remote unauthenticated attacker may be able to bypass authentication by sending specially crafted packets and connect to the products. The reason why it ranks last is because of what this vulnerability offers to the attacker, which is less risky than other vulnerabilities.