Threat Intelligence Report:

CVE-2023-6942& CVE-2023-6943: The systems affected by these vulnerabilities are the systems developed by Mitsubishi Electric, which are responsible for the control of all kinds of vehicles in factories. By exploiting these vulnerabilities, the attacker can first bypass the system's remote authentication step by sending specially crafted packets and gain unauthorized access to the system. Then, by exploiting the remote code execution vulnerability then the attacker invokes the malicious library to disrupt the functionality of the target system. this allows the attacker to manipulate the target system at will.

IOC'S: There is no IOC share specifically for this vulnerabilities, but there are some things you can do to detect exploitation of these vulnerabilities. Monitoring changes in functions exported from authentication-related system DLLs. Monitor newly created logon behaviors between systems that share accounts, such as user, administrator, or service accounts. Monitor for API calls to OpenProcess that can be used to manipulate lsass.exe running on a domain controller. Monitor for unexpected processes interacting with the authentication process on a domain controller to bypass the typical authentication mechanisms and enable access to accounts. Monitor for third-party application logging, messaging, and/or other artifacts that may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. In addition to network level detections, endpoint logging and instrumentation can be useful for detection. Attacks targeting web applications may generate logs in the web server, application server, and/or database server that can be used to identify the type of attack, possibly before the impact is felt. Externally monitor the availability of services that may be targeted by an Endpoint DoS. Monitor network traffic.

CVE-2024-21917: The Rockwell Automation FactoryTalk Service Platform, which is affected by this vulnerability, is a cyber security platform for factories. In short, this vulnerability allows the hacking of one FTSP system to easily hack other FTSP systems. An example attack scenario where this vulnerability is exploited; A hacker accesses an FTSP service in a factory and obtains a service token. This token contains the identity and authorizations of the service.

The hacker sends this token to another FTSP directory and accesses the data in the directory. This data contains the status, settings and users of machines and devices in the factory.

The hacker can read, modify or delete this data. For example, the hacker can disrupt the production process in the factory, malfunction or stop machines and devices, hijack or delete user accounts.

The hacker is authorized with the FTSP service token to perform these actions without any authentication or leaving any traces. Therefore, factory management or security personnel may not notice the presence or activities of the hacker.

The IoCs of this vulnerability are:

- Service token used to access the FTSP directory of the affected device.
- API requests used to read or modify data in the affected device's FTSP directory.
- Abnormal service token or API activities seen in the affected device's syslog.