|  |  |
| --- | --- |
| Title | Numerous Unauthorized Accesses in Scheduling Tasks of the Tempo Big Data Analysis Platform |
| Severity Level | High Risk |
| Incident URLs: | /cloud-system-job/jobinfo/pageList // Query all scheduling task lists  /cloud-system-job/jobinfo/add // Add scheduling tasks  /cloud-system-job/jobinfo/remove // Delete scheduling tasks  /cloud-system-job/jobinfo/start // Run scheduling tasks |
| Description | The platform's scheduling task interfaces lack proper authorization checks, allowing attackers to send data packets and perform arbitrary operations such as adding, deleting, or running tasks across all management interfaces. This unauthorized access could lead to malicious manipulation of the system, adversely affecting normal business operations.  Vulnerability Verification:：  After setting up the Tempo Big Data Analysis Platform, access the system management and click on scheduling task management.  Using Burp Suite for packet capture, it was observed that all authorization request headers were removed, yet access to the interface was still successful, allowing retrieval of the system's scheduling task list.    Creating a scheduling task.  Deleting a scheduling task. |