Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 310 **22-07-2024**

Name: Multiple Apache Products Vulnerabilities

Threat Classification: Vulnerability

Affected Software / Area:

- Apache CXF before 4.0.5, 3.6.4 and 3.5.9 version
- Apache Airflow 2.4.0, and versions before 2.9.3
- Apache StreamPipes version 0.93.0

Summary:

Several critical vulnerabilities have been discovered in Apache products, affecting CXF, Airflow, and StreamPipes. These vulnerabilities, identified as **CVE-2024-32007**, **CVE-2024-41172**, **CVE-2024-39877**, and **CVE-2024-31411**, can lead to denial of service or arbitrary code execution. Exploits involve sending specially crafted requests that leverage improper input validation or memory flaws.

Severity	**High**
Attack Vector	**DOS**

Recommendations:

- It is recommended that Immediately apply patches available on Apache Website.

- https://cxf.apache.org/download.html
- https://streampipes.apache.org/download/
- https://airflow.apache.org/docs/apache-airflow/stable/release_notes.html#airflow-2-9-3-2024-07-15

- Regularly monitor systems for unusual activity that might indicate an attempt to exploit these vulnerabilities.
- Deploy and maintain robust endpoint protection solutions to detect and prevent the execution of malicious code.
- Establish a proactive patch management process to ensure timely deployment of security updates for all software and systems.
- In case of any incident, please report to this office, through PTA CERT Portal and email.