



Home > Submit > 782200

Submit #782200: FedML-AI FedML <=0.8.9 Path Traversal

Title	FedML-AI FedML <=0.8.9 Path Traversal
Description	A path traversal vulnerability (CVE-22) exists in the Android client of FedML. The client processes MQTT messages as task instructions and uses the dataSet parameter to construct filesystem paths without validation. An attacker who can publish or tamper with MQTT messages can supply crafted path traversal payloads (e.g., <code>../../../../</code>) to cause the client to access and enumerate arbitrary directories within the app's accessible filesystem.
Source	https://github.com/AnalogyC0de/public_exp/issues/25
User	Analogy (UID 93358)
Submission	03/13/2026 09:40 AM (18 days ago)
Moderation	04/04/2026 08:40 AM (17 days later)
Status	Accepted
VulDB entry	#782200 [FedML-AI FedML up to 0.8.9 MQTT Message FileUtils.java dataSet path traversal]
Points	20

Community Content

Submissions are made by [VulDB community users](#). VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- [Submission Policy](#)
- [Data Processing](#)
- [CVE Handling](#)