COMMUNITY CONTENT

Submit #782201: FedML-AI FedML <= 0.8.9 Remote Code Execution

Title	FedML-AI FedML <= 0.8.9 Remote Code Execution
Description	Fedml is vulnerable to Remote Code Execution (RCE) due to unsafe deserialization in its gRPC communication manager. The application's gRPC server is exposed to all network interfaces (x.x.x.x) via an insecure port without requiring authentication. Network messages received through the sendMessage() RPC are passed directly to pickle.loads(). This allows an unauthenticated remote attacker to send a maliciously crafted Python pickle payload, which upon deserialization executes arbitrary code on the affected federated learning node.
Source	https://github.com/AnalogyC0de/public_exp/issues/26
User	Ana1Ogy (UID 93358)
Submission	03/18/2026 09:44 AM (18 days ago)
Moderation	04/04/2026 08:41 AM (17 days later)
Status	Accepted
VulDB entry	[FedML-AI FedML up to 0.8.9 gRPC server grpc_server.py sendMessage deserialization]
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