New issue

Remote Code Execution via gRPC Pickle Deserialization in Fedml #26

Open

AnalogyC0de opened 3 weeks ago Owner

Remote Code Execution via gRPC Pickle Deserialization in Fedml

Identification

- **Project:** Fedml
- **Repository:** https://github.com/FedML-AI/FedML
- **Affected Version/Commit:** <=0.8.9

CVE 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 (`0.0.0.0`) 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.

Affected Component

- **File(s):** `grpc_server.py`, `grpc_comm_manager.py`
- **Function / Method:** `sendMessage()`, `pickle.loads()`, `add_insecure_port()`
- **Entry Point:** gRPC network listener on `0.0.0.0:8890+`

Reproduction Summary

1. An unauthenticated attacker connects to the exposed FedML gRPC server (default port `8890+`).
2. The attacker sends a maliciously crafted serialized payload to the `sendMessage()` RPC endpoint.
3. The server processes the network request and passes the unvalidated input to `pickle.loads()`.
4. The malicious payload is deserialized, achieving arbitrary Remote Code Execution on the node.

Technical Details

```
Vulnerable Components & Data Flow:
- Network Exposure: The gRPC server listens on 0.0.0.0 using add_insecure_port() for po
8890+
- Entry Point: grpc_server.py:26-39 handles the sendMessage() RPC
- Sink: grpc_comm_manager.py:136 executes pickle.loads() on the incoming message
- Authentication: None. Any network client can communicate with the gRPC server.
```


Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants