VDB-355289 · CVE-2026-5536 · GCVE-100-355289

FEDML-AI FEDML UP TO 0.8.9 GRPC SERVER GRPC_SERVER.PY SENDMESSAGE DESERIALIZATION

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

7.1 | $0-$5k | 1.76

Summary

A vulnerability marked as critical has been reported in FedML-AI FedML up to 0.8.9. Affected by this vulnerability is the function `sendMessage` of the file *grpc_server.py* of the component *gRPC server*. The manipulation leads to deserialization. This vulnerability is traded as CVE-2026-5536. It is possible to initiate the attack remotely. There is no exploit available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in FedML-AI FedML up to 0.8.9 and classified as critical. This issue affects the function `sendMessage` of the file *grpc_server.py* of the component *gRPC server*. The manipulation with an unknown input leads to a deserialization vulnerability. Using CWE to declare the problem leads to CWE-502. The product deserializes untrusted data without sufficiently verifying that the resulting data will be valid. Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-5536. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details are known, but no exploit is available. The price for an exploit might be around USD $0-$5k at the moment (estimation calculated on 04/04/2026).

The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The entry VDB-195324 is related to this item.

Product

Type

- Artificial Intelligence Software

Vendor

- FedML-AI

Name

- FedML

Version

- 0.8.0
- 0.8.1
- 0.8.2
- 0.8.3
- 0.8.4
- 0.8.5
- 0.8.6
- 0.8.7
- 0.8.8
- 0.8.9

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 7.3
VulDB Meta Temp Score: 7.1

VulDB Base Score: 7.3
VulDB Temp Score: 7.1
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Deserialization
CWE: CWE-502 / CWE-20
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Status: Not defined
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/04/2026		Advisory disclosed
04/04/2026	+0 days	VulDB entry created
04/04/2026	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5536 (🔒)
GCVE (CVE): GCVE-0-2026-5536
GCVE (VulDB): GCVE-100-355289
See also: 🔒

Entry

Created: 04/04/2026 08:46 AM
Changes: 04/04/2026 08:46 AM (54)
Complete: 🔍
Submitter: Ana10gy
Cache ID: 51:5D1:179

Submit

Accepted

- Submit #782201: FedML-AI FedML <= 0.8.9 Remote Code Execution (by Ana10gy)

Discussion

No comments yet. Languages: en.

Please log in to comment.