VDB-355288 · CVE-2026-5535 · GCVE-100-355288

FEDML-AI FEDML UP TO 0.8.9 MQTT MESSAGE FILEUTILS.JAVA DATASET PATH TRAVERSAL

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

3.9 | $0-$5k | 1.86

Summary

A vulnerability labeled as critical has been found in FedML-AI FedML up to 0.8.9. Affected is an unknown function of the file *FileUtils.java* of the component *MQTT Message Handler*. Executing a manipulation of the argument *dataSet* can lead to path traversal. This vulnerability appears as CVE-2026-5535. The attack may be performed from remote. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability has been found in FedML-AI FedML up to 0.8.9 and classified as problematic. This vulnerability affects an unknown part of the file *FileUtils.java* of the component *MQTT Message Handler*. The manipulation of the argument `dataSet` with an unknown input leads to a path traversal vulnerability. The CWE definition for the vulnerability is CWE-22. The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. As an impact it is known to affect confidentiality.

The advisory is shared for download at github.com. This vulnerability was named CVE-2026-5535. The exploitation appears to be easy. The attack can be initiated remotely. Technical details and also a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1006.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. 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.

See VDB-226896, VDB-239438 and VDB-282555 for similar entries.

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: 4.3
VulDB Meta Temp Score: 3.9

VulDB Base Score: 4.3
VulDB Temp Score: 3.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Path traversal
CWE: CWE-22
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
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-2026-5535 (🔒)
GCVE (CVE): GCVE-0-2026-5535
GCVE (VulDB): GCVE-100-355288
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 08:45 AM
Changes: 04/04/2026 08:45 AM (58)
Complete: 🔍
Submitter: Ana10gy
Cache ID: 20:0CC:179

Submit

Accepted

- Submit #782200: FedML-AI FedML <=0.8.9 Path Traversal (by Ana10gy)

Discussion

No comments yet. Languages: en.

Please log in to comment.