



VDB-354658 · CVE-2026-5327 · ISSUE 15

EFFORTHYE FAST-FILESYSTEM-MCP UP TO 3.5.1 SRC/INDEX.TS HANDLEGETDISKUSAGE COMMAND INJECTION

CVSS Meta Temp Score ⓘ

6.0

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

1.22-

Summary

A vulnerability labeled as **critical** has been found in [efforthye fast-filessystem-mcp up to 3.5.1](#). The impacted element is the function `handleGetDiskUsage` of the file `src/index.ts`. Executing a manipulation can lead to command injection. This vulnerability appears as [CVE-2026-5327](#). The attack may be performed from remote. In addition, an exploit is available. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability has been found in [efforthye fast-filessystem-mcp up to 3.5.1](#) and classified as **critical**. This vulnerability affects the function `handleGetDiskUsage` of the file `src/index.ts`. The manipulation with an unknown input leads to a command injection vulnerability. The CWE definition for the vulnerability is [CWE-77](#). The product constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is available at [github.com](#). This vulnerability was named [CVE-2026-5327](#). The exploitation appears to be easy. The attack can be initiated remotely. Technical details and also a public exploit are known. This vulnerability is assigned to [T1202](#) by the MITRE ATT&CK project.

It is possible to download the exploit at [github.com](#). It is declared as proof-of-concept. The project was informed of the problem early through an issue report but has not responded yet.

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

See [VDB-169422](#), [VDB-222729](#), [VDB-344765](#) and [VDB-348559](#) for similar entries.

Product

Vendor

- [efforthye](#)

Name

- [fast-filesystem-mcp](#)

Version

- [3.5.0](#)
- [3.5.1](#)

Website

- Product: <https://github.com/efforthye/fast-filesystem-mcp/>

CPE 2.3

- 
- 

CPE 2.2

- 
- 

CVSSv4

VulDB Vector: 

VulDB Reliability: 

CVSSv3

VulDB Meta Base Score: 6.3

VulDB Meta Temp Score: 6.0

VulDB Base Score: 6.3

VulDB Temp Score: 6.0

VulDB Vector: 

VulDB Reliability: 

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Command injection

CWE: [CWE-77](#) / [CWE-74](#) / [CWE-707](#)

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

04/01/2026		Advisory disclosed
04/01/2026	+0 days	VulDB entry created
04/01/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: [15](#)

Status: Confirmed

CVE: [CVE-2026-5327](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5327](#)

GCVE (VulDB): [GCVE-100-354658](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🔒

Entry

Created: 04/01/2026 03:32 PM

Changes: 04/01/2026 03:32 PM (57)

Complete: 🔍

Submitter: [Yinci Chen](#)

Cache ID: 48:815:179

Submit

Accepted

- [Submit #780776](#): efforthye fast-filessystem-mcp <= 3.5.1 Command Injection (by Yinci Chen)

Discussion

No comments yet. Languages: en.

Please log in to comment.