VDB-307362 · CVE-2025-4258 · GCVE-100-307362

ZHANGYANBO2007 YOUKEFU UP TO 4.2.0 MEDIACONTROLLER.JAVA UPLOAD IMGFILE UNRESTRICTED UPLOAD

A vulnerability, which was classified as critical, was found in zhangyanbo2007 youkefu up to 4.2.0. Affected is the function `upload` of the file *\youkefu-master\src\main\java\com\ukefu\webim\web\handler\resource\MediaController.java*. The manipulation of the argument `imgFile` with an unknown input leads to a unrestricted upload vulnerability. CWE is classifying the issue as CWE-434. The product allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is traded as CVE-2025-4258. The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known. This vulnerability is assigned to T1608.002 by the MITRE ATT&CK project.

The exploit is shared for download at github.com. It is declared as proof-of-concept.

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

The entries VDB-291277, VDB-295019, VDB-298102 and VDB-299221 are pretty similar.

Product

Vendor

- zhangyanbo2007

Name

- youkefu

Version

- 4.0
- 4.1
- 4.2.0

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 6.0

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 6.3
CNA Vector: 🔒

CVSSv2

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

Exploiting

Class: Unrestricted upload
CWE: CWE-434 / CWE-284 / CWE-266
CAPEC: 🔒
ATT&CK: 🔒

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

05/04/2025		Advisory disclosed
05/04/2025	+0 days	VulDB entry created
05/05/2025	+1 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4258 (🔒)
GCVE (CVE): GCVE-0-2025-4258
GCVE (VulDB): GCVE-100-307362

scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/04/2025 09:07 AM
Updated: 05/05/2025 01:21 PM
Changes: 05/04/2025 09:07 AM (56), 05/04/2025 09:13 AM (1), 05/05/2025 05:49 AM (30), 05/05/2025 01:21 PM (1)
Complete: 🔍
Submitter: Fc04dB
Cache ID: 5:C49:101

Submit

Accepted

- Submit #562848: https://github.com/zhangyanbo2007/youkefu ukefu 1.0 Unrestricted Upload (by Fc04dB)

Discussion

No comments yet. Languages: en.

Please log in to comment.