VDB-306797 · CVE-2025-4178 · GCVE-100-306797

XIAOWEI1118 JAVA_SERVER UP TO 11A5BAC8F4BA1C17E4BC1B27CAD6D24868500E3A ON WINDOWS FILE UPLOAD API FOODCONTROLLER.JAVA PATH TRAVERSAL

A vulnerability was found in xiaowei1118 java_server up to 11a5bac8f4ba1c17e4bc1b27cad6d24868500e3a on Windows and classified as critical. This issue affects an unknown functionality of the file */src/main/java/com/changyu/foryou/controller/FoodController.java* of the component *File Upload API*. The manipulation with an unknown input leads to a path traversal vulnerability. Using CWE to declare the problem leads to 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. Impacted is integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2025-4178. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1006 for this issue.

The exploit is available 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.

Product

Type

- Programming Language Software

Vendor

- xiaowei1118

Name

- java_server

Version

- 11a5bac8f4ba1c17e4bc1b27cad6d24868500e3a

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: 5.4
VulDB Meta Temp Score: 5.1

VulDB Base Score: 5.4
VulDB Temp Score: 4.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 5.4
CNA Vector: 🔒

CVSSv2

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

Exploiting

Class: Path traversal
CWE: CWE-22
CAPEC: 🔒

ATT&CK: 🔒

Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒

EPSS Score: 🔒
EPSS Percentile: 🔒

Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/01/2025		Advisory disclosed
05/01/2025	+0 days	VulDB entry created
05/02/2025	+1 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4178 (🔒)
GCVE (CVE): GCVE-0-2025-4178
GCVE (VulDB): GCVE-100-306797
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 05/01/2025 02:44 PM
Updated: 05/02/2025 10:45 AM
Changes: 05/01/2025 02:44 PM (58), 05/02/2025 10:45 AM (30)
Complete: 🔍
Submitter: ShenxiuSecurity
Cache ID: 5:A57:101

Submit

Accepted

- Submit #561794: xiaowei1118 java_server master branch Path Traversal (by ShenxiuSecurity)

Discussion

No comments yet. Languages: en.

Please log in to comment.