VDB-306795 · CVE-2025-4175 · GCVE-100-306795

ALANBINU007 SPRING-BOOT-ADVANCED-PROJECTS UP TO 3.1.3 UPLOAD PROFILE API ENDPOINT USERPROFILECONTROLLER.JAV UPLOADUSERPROFILEIMAGE FILE PATH TRAVERSAL

A vulnerability, which was classified as critical, was found in AlanBinu007 Spring-Boot-Advanced-Projects up to 3.1.3. This affects the function `uploadUserProfileImage` of the file */Spring-Boot-Advanced-Projects-main/Project-4.SpringBoot-AWS-S3/backend/src/main/java/com/urunov/profile/UserProfileController.jav* of the component *Upload Profile API Endpoint*. The manipulation of the argument `file` with an unknown input leads to a path traversal vulnerability. CWE is classifying the issue as 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. This is going to have an impact on confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is uniquely identified as CVE-2025-4175. The exploitability is told to be easy. It is possible to initiate the attack remotely. Technical details and a public exploit are known. The attack technique deployed by this issue is T1006 according to MITRE ATT&CK.

The exploit is shared for download 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.

Similar entries are available at VDB-303688, VDB-304592, VDB-304593 and VDB-304599.

Product

Type

- Project Management Software

Vendor

- AlanBinu007

Name

- Spring-Boot-Advanced-Projects

Version

- 3.1.0
- 3.1.1
- 3.1.2
- 3.1.3

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

[redacted]

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: 🔒

[redacted]

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-2025-4175 (🔒)
GCVE (CVE): GCVE-0-2025-4175
GCVE (VulDB): GCVE-100-306795
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/01/2025 02:34 PM
Updated: 05/02/2025 10:45 AM
Changes: 05/01/2025 02:34 PM (59), 05/02/2025 10:45 AM (30)
Complete: 🔍
Submitter: ShenxiuSecurity
Cache ID: 5:4C0:101

Submit

Accepted

- Submit #561760: AlanBinu007 Spring-Boot-Advanced-Projects v3.1.3 Path Traversal (by ShenxiuSecurity)

Discussion

No comments yet. Languages: en.

Please log in to comment.