VDB-308274 · CVE-2025-4529 · GCVE-100-308274

SEEYON ZHIYUAN OA WEB APPLICATION SYSTEM 8.1 SP2 ZIP FILE M3CORECONTROLLER.CLASS DOWNLOAD NAME PATH TRAVERSAL

A vulnerability was found in Seeyon Zhiyuan OA Web Application System 8.1 SP2. It has been classified as problematic. Affected is the function `download` of the file *seeyon\opt\Seeyon\A8\ApacheJetspeed\webapps\seeyon\WEB-INF\lib\seeyon-apps-m3.jar!\com\seeyon\apps\m3\core\controller\M3CoreController.class* of the component *ZIP File Handler*. The manipulation of the argument `name` 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.

The advisory is available at wx.mail.qq.com. This vulnerability is traded as CVE-2025-4529. 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 T1006 by the MITRE ATT&CK project.

The exploit is shared for download at wx.mail.qq.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-135237, VDB-140656, VDB-192967 and VDB-240146 are related to this item.

Product

Vendor

- Seeyon

Name

- Zhiyuan OA Web Application System

Version

- 8.1 SP2

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: 4.3
VulDB Meta Temp Score: 4.1

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

CNA Base Score: 4.3
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: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/10/2025		Advisory disclosed
05/10/2025	+0 days	VulDB entry created
05/11/2025	+1 days	VulDB entry last update

Sources

Advisory: wx.mail.qq.com
Status: Not defined

CVE: CVE-2025-4529 (🔒)
GCVE (CVE): GCVE-0-2025-4529
GCVE (VulDB): GCVE-100-308274
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/10/2025 07:38 AM
Updated: 05/11/2025 07:04 AM
Changes: 05/10/2025 07:38 AM (57), 05/11/2025 07:04 AM (30)
Complete: 🔍
Submitter: caichaoxiong
Cache ID: 5:717:101

Submit

Accepted

- Submit #565379: Seeyon Zhiyuan OA Web Application System V8.1 SP2 Path Traversal Vulnerability (by caichaoxiong)

Discussion

No comments yet. Languages: en.

Please log in to comment.