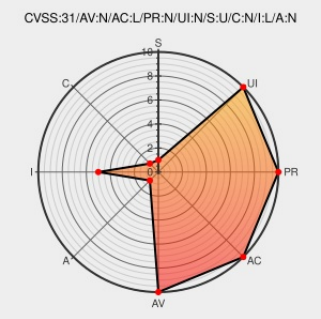
CVE-2021-4314

Published on: Not Yet Published

Last Modified on: 01/26/2023 06:33:00 PM UTC

CVE-2021-4314

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Zowe Api Mediation Layer from Linuxfoundation contain the following vulnerability:

It is possible to manipulate the JWT token without the knowledge of the JWT secret and authenticate without valid JWT token as any user. This is happening only in the situation when zOSMF doesn't have the APAR PH12143 applied. This issue affects: 1.16 versions to 1.19. What happens is that the services using the ZAAS client or the API ML API to query will be deceived into believing the information in the JWT token is valid when it isn't. It's possible to use this to persuade the southbound service that different user is authenticated.

CVE-2021-4314 has been assigned by zowe-security@lists.openmainframeproject.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Open Mainframe Project** - **Zowe** version **= 1.16.0**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	LOW	NONE

CVE References

Description	Tags	Link
GitHub - zowe/api-layer: The API Mediation Layer provides a single point of access for mainframe service REST APIs.	github.com text/html	MISC github.com/zowe/api-layer/

comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

It is possible to manipulate the JWT token without the knowledge of the JWT secret and authenticate without valid JWT…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Zowe Api Mediation Layer	All	All	All	All

cpe:2.3:a:linuxfoundation:zowe_api_mediation_layer:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-4314 : It is possible to manipulate the JWT token without the knowledge of the JWT secret and authenticate… twitter.com/i/web/status/1…	2023-01-18 16:04:50
/r/netcve	CVE-2021-4314	2023-01-18 16:39:15

← Previous ID

Next ID→