



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/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

[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 →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)