



CVE-2022-22733

Published on: 01/20/2022 12:00:00 AM UTC

Last Modified on: 01/26/2022 04:37:00 PM UTC

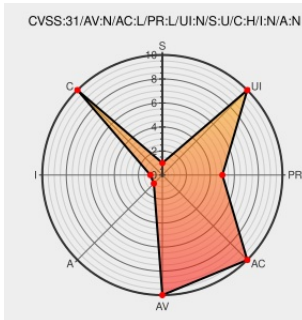
CVE-2022-22733

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Shardingsphere Elasticjob-ui](#) from [Apache](#) contain the following vulnerability:

Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache ShardingSphere ElasticJob-UI allows an attacker who has guest account to do privilege escalation. This issue affects Apache ShardingSphere ElasticJob-UI Apache ShardingSphere ElasticJob-UI 3.x version 3.0.0 and prior versions.

CVE-2022-22733 has been assigned by security@apache.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache ShardingSphere ElasticJob-UI** version <= 3.0.0

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
No Description Provided	lists.apache.org	MISC

oss-security - CVE-2022-22733: Apache ShardingSphere ElasticJob-UI: Access-Token in ElasticJob UI causes password disclosure

www.openwall.com
text/html

MLIST [oss-security] 20220120 CVE-2022-22733: Apache ShardingSphere ElasticJob-UI: Access-Token in ElasticJob UI causes password disclosure

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

Apache ShardingSphere ElasticJob-UI Privilege Escalation & RCE Exploit

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Shardingsphere Elasticjob-ui	3.0.0	-	All	All
Application	Apache	Shardingsphere Elasticjob-ui	3.0.0	alpha	All	All
Application	Apache	Shardingsphere Elasticjob-ui	3.0.0	beta	All	All
Application	Apache	Shardingsphere Elasticjob-ui	3.0.0	rc1	All	All

cpe:2.3:a:apache:shardingsphere_elasticjob-ui:3.0.0:-:*:*:*:*:

cpe:2.3:a:apache:shardingsphere_elasticjob-ui:3.0.0:alpha:*:*:*:*:

cpe:2.3:a:apache:shardingsphere_elasticjob-ui:3.0.0:beta:*:*:*:*:

cpe:2.3:a:apache:shardingsphere_elasticjob-ui:3.0.0:rc1:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-22733 : Exposure of Sensitive Information to an Unauthorized Actor vulnerability in #Apache ShardingSphere... twitter.com/i/web/status/1...	2022-01-20 10:31:47
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-22733 Description: Exposure of Sensitive Information to an Unauthorized... twitter.com/i/web/status/1...	2022-01-20 11:56:11
 /r/netcve	CVE-2022-22733	2022-01-20 11:38:24

← Previous ID

Next ID →

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](#)