

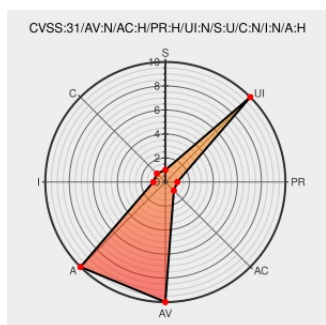


CVE-2022-31080

Published on: Not Yet Published

Last Modified on: 07/24/2023 01:16:00 PM UTC

CVE-2022-31080 - advisory for GHSA-6wvc-6pww-qr4r

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Kubeedge](#) from [Linuxfoundation](#) contain the following vulnerability:

KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, a large response received by the viaduct WSCClient can cause a DoS from memory exhaustion. The entire body of the response is being read into memory which could allow an

attacker to send a request that returns a response with a large body. The consequence of the exhaustion is that the process which invokes a WSCClient will be in a denial of service. The software is affected If users who are authenticated to the edge side connect to `cloudhub` from the edge side through WebSocket protocol. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. There are currently no known workarounds.

CVE-2022-31080 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: kubeedge - kubeedge version = 1.11.0

Affected Vendor/Software: kubeedge - kubeedge version >= 1.10.0, < 1.10.2

Affected Vendor/Software: kubeedge - kubeedge version < 1.9.4

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	NONE	NONE	HIGH

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Websocket Client in package Viaduct: DoS from large response message · Advisory · kubeedge/kubeedge · GitHub	github.com text/html	 CONFIRM github.com/kubeedge/kubeedge/security/advisories/GHSA-6wvc-6pww-qr4r

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Kubeedge	All	All	All	All

```
cpe:2.3:a:linuxfoundation:kubeedge:*:*:*:*:*:*
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-31080 : KubeEdge is an open source system for extending native containerized application orchestration cap... twitter.com/i/web/status/1...	2022-07-11 20:56:03
 /r/netcve	CVE-2022-31080	2022-07-11 21:38:15

[← 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](#)