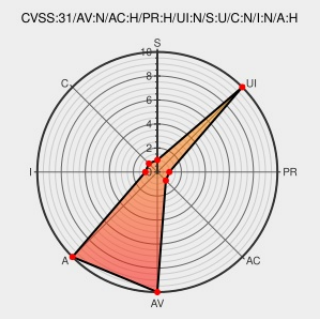
CVE-2022-31080

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 WSClient 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 WSClient 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

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→