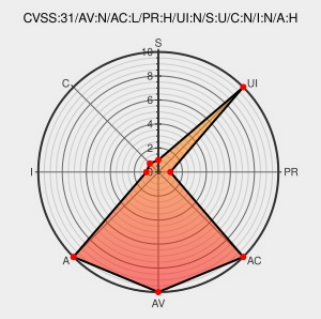
CVE-2022-31075

Published on: Not Yet Published

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

CVE-2022-31075 - advisory for GHSA-x3px-2p95-f6jr

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, EdgeCore may be susceptible to a DoS attack on CloudHub if an attacker was to send a well-crafted HTTP request to `/edge.crt`. If an attacker can send a well-crafted HTTP request to CloudHub, and that request has a very large body, that request can crash the HTTP service through a memory exhaustion vector. The request body is being read into memory, and a body that is larger than the available memory can lead to a successful attack. Because the request would have to make it through authorization, only authorized users may perform this attack. The consequence of the exhaustion is that CloudHub will be in denial of service. KubeEdge is affected only when users enable the CloudHub module in the file `cloudcore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the CloudHub switch in the config file `cloudcore.yaml`.

CVE-2022-31075 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **kubeedge** - **kubeedge** version **< 1.9.4**

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

Affected Vendor/Software: **kubeedge** - **kubeedge** version **= 1.11.0**

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	NONE	NONE	HIGH

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
DoS when signing the CSR from EdgeCore · Advisory · kubeedge/kubeedge · GitHub	github.com text/html	CONFIRM github.com/kubeedge/kubeedge/security/advisories/GHSA-x3px-2p95-f6jr

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-2022-31075 : KubeEdge is an open source system for extending native containerized application orchestration cap… twitter.com/i/web/status/1…	2022-07-11 20:22:39
/r/netcve	CVE-2022-31075	2022-07-11 21:38:13

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report