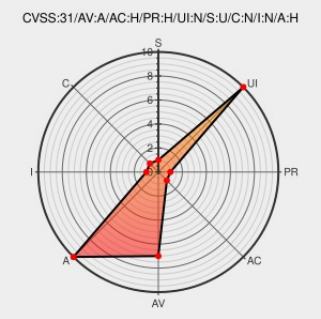
CVE-2022-31076

Published on: Not Yet Published

Last Modified on: 07/07/2022 07:28:00 PM UTC

CVE-2022-31076 - advisory for GHSA-8f4f-v9x5-cg6j

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Kubeedge from Linuxfoundation contain the following vulnerability:

KubeEdge is built upon Kubernetes and extends native containerized application orchestration and device management to hosts at the Edge. In affected versions a malicious message can crash CloudCore by triggering a nil-pointer dereference in the UDS Server. Since the UDS Server only communicates with the CSI Driver on the cloud side, the attack is limited to the local host network. As such, an attacker would already need to be an authenticated user of the Cloud. Additionally it will be affected only when users turn on the unixsocket switch in the config file cloudcore.yaml. This bug has been fixed in Kubeedge 1.11.0, 1.10.1, and 1.9.3. Users should update to these versions to resolve the issue. Users unable to upgrade should sisable the unixsocket switch of CloudHub in the config file cloudcore.yaml.

CVE-2022-31076 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **kubeedge** - **kubeedge** version **< 1.9.3**

Affected Vendor/Software: **kubeedge** - **kubeedge** version **>= 1.10.0, < 1.10.1**

CVSS3 Score: 5.7 - MEDIUM

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

CVSS2 Score: 2.7 - LOW

Access Vector	Access Complexity	Authentication

ADJACENT_NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
CloudCore UDS Server: Malicious Message can crash CloudCore · Advisory · kubeedge/kubeedge · GitHub	github.com text/html	CONFIRM github.com/kubeedge/kubeedge/security/advisories/GHSA-8f4f-v9x5-cg6j
fix fuzzer extract message error by vincentgoat · Pull Request #3899 · kubeedge/kubeedge · GitHub	github.com text/html	MISC github.com/kubeedge/kubeedge/pull/3899/commits/5d60ae9eabd6b6b7afe38758e19bbe8137664701

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
Application	Linuxfoundation	Kubeedge	1.10.0	-	All	All
Application	Linuxfoundation	Kubeedge	1.10.0	beta0	All	All

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

cpe:2.3:a:linuxfoundation:kubeedge:1.10.0:-:*:*:*:*:*:*:

cpe:2.3:a:linuxfoundation:kubeedge:1.10.0:beta0:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31076 : KubeEdge is built upon Kubernetes and extends native containerized application orchestration and d… twitter.com/i/web/status/1…	2022-06-27 20:14:25
@LinInfoSec	Kubernetes - CVE-2022-31076: github.com/kubeedge/kubee…	2022-06-27 23:05:59

/r/netcve	CVE-2022-31076	2022-06-27 22:38:52

← Previous ID

Next ID→