kubeedge / **kubeedge** Public

Code Issues 331 Pull requests 65 Discussions Actions Projects ...

CloudCore UDS Server: Malicious Message can crash CloudCore

Moderate **kubeedge-bot** published **GHSA-8f4f-v9x5-cg6j** on Jun 24

Package

KubeEdge (Go)

Affected versions	Patched versions
<=1.10.0, 1.9.2, 1.8.2	1.11.0, 1.10.1, 1.9.3

Description

Impact

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.

It will be affected only when users turn on the unixsocket switch in the config file `cloudcore.yaml` as below:

```
modules:
  cloudHub:
    ...
    unixsocket:
      address: xxx
      enable: true
```

Patches

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.

Workarounds

Disable the unixsocket switch of CloudHub in the config file `cloudcore.yaml` .

References

NA

Credits

Thanks David Korczynski and Adam Korczynski of ADA Logics for responsibly disclosing this issue in accordance with the kubeedge security policy during a security audit sponsored by CNCF and facilitated by OSTIF.

For more information

If you have any questions or comments about this advisory:

- Open an issue in KubeEdge repo
- To make a vulnerability report, email your vulnerability to the private cncf-kubeedge-security@lists.cncf.io list with the security details and the details expected for KubeEdge bug reports.

Notes: This vulnerability was found by fuzzing KubeEdge by way of OSS-Fuzz.

Severity

Moderate 4.2 / 10

CVSS base metrics

Attack vector	**Adjacent**
Attack complexity	**High**
Privileges required	**High**
User interaction	**None**
Scope	**Unchanged**
Confidentiality	**None**
Integrity	**None**
Availability	**High**

CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2022-31076

Weaknesses

No CWEs

Credits

DavidKorczynski

AdamKorcz