kubeedge / **kubeedge** Public

Code | Issues 331 | Pull requests 65 | Discussions | Actions | Projects | ···

Edge ServiceBus module: DoS by exhausting memory of node with http request containing large body

Moderate **kevin-wangzefeng** published **GHSA-vwm6-qc77-v2rh** on Jul 11

Package

KubeEdge (Go)

Affected versions	Patched versions
<=1.11.0, 1.10.1, 1.9.3	1.11.1, 1.10.2, 1.9.4

Description

Impact

The ServiceBus server on the edge side may be susceptible to a DoS attack if an HTTP request containing a very large Body is sent to it.
It is possible for the node to be exhausted of memory. The consequence of the exhaustion is that other services on the node, e.g. other containers, will be unable to allocate memory and thus causing a denial of service.
Malicious Apps which by accident pulled by users on the host and have the access to send HTTP requests to localhost may make an attack. It will be affected only when users enable the `ServiceBus` module in the config file `edgecore.yaml` as below:

```
modules:
  ...
  serviceBus:
    enable: true
```

Patches

This bug has been fixed in Kubeedge 1.11.1, 1.10.2, 1.9.4. Users should update to these versions to resolve the issue.

Workarounds

Disable the ServiceBus module in the config file `edgecore.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.

Severity

Moderate 6.5 / 10

CVSS base metrics

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

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

CVE ID

CVE-2022-31073

Weaknesses

No CWEs

Credits

DavidKorczynski

AdamKorcz