



# Bug 2272339 (CVE-2024-5037) - CVE-2024-5037 openshift/telemeter: iss check during JWT authentication can be bypassed

**Keywords:**

**Reported:** 2024-03-31 00:33 UTC by Robb Gatica

**Status:** NEW

**Modified:** 2025-03-17 23:44 UTC (History)

**Alias:** CVE-2024-5037

**CC List:** 8 users (show)

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Version:** unspecified

**Environment:**

**Hardware:** All

**Last Closed:**

**OS:** Linux

**Embargoed:**

**Priority:** high

**Severity:** high

**Target Milestone:** ---

**Assignee:** Product Security

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:**

**Blocks:** 2272338

**TreeView+** depends on / blocked

Attachments	(Terms of Use)

### Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHSA-2024:4151</a>	0	None	None	None	2024-07-02 19:32:48 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:4156</a>	0	None	None	None	2024-07-03 11:29:58 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:4329</a>	0	None	None	None	2024-07-11 11:54:29 UTC

Red Hat Product Errata	<a href="#">RHSA-2024:4484</a>	0	None	None	None	2024-07-17 01:37:10 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:5200</a>	0	None	None	None	2024-08-19 05:40:43 UTC

Robb Gatica 2024-03-31 00:33:22 UTC

[Description](#)**Description:**

When verifying the iss field, telemeter uses ``strings.Split(tokenData, ".")`` to extract the payload, which means that the user should submit a Compact type JWS Token. However, go-jose's ``jwt.ParseSigned(tokenData)`` also supports authenticating JWS Token of JSON type. That means if the attacker submits a Token like:

```

...
{
  "fakeiss": ".eyJpc3MiOiJhY2NvdW50cy5nb29nbGUuY29tIn0.",
  "protected": "",
  "header": "",
  "payload": "",
  "signature": ""
}
...

```

The attacker can forge a token issued by Google to pass the verification(for example). If two server use the same pair of key, the attacker can use the token from the first server to deceive the second server, and cause the privilege escape. The original reporter has raised this issue to Kubernetes, and they have fixed this problem:

<https://github.com/kubernetes/kubernetes/pull/123540>

---

<https://github.com/openshift/telemeter>

Version: 4.17

Related Code:

[https://github.com/openshift/telemeter/blob/a9417a6062c3a31ed78c06ea3a0613a52f2029b2/pkg/authorize/jwt/client\\_authorizer.go#L78](https://github.com/openshift/telemeter/blob/a9417a6062c3a31ed78c06ea3a0613a52f2029b2/pkg/authorize/jwt/client_authorizer.go#L78)

errata-xmlrpc 2024-07-02 19:32:47 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.15

Via [RHSA-2024:4151](#) <https://access.redhat.com/errata/RHSA-2024:4151>

errata-xmlrpc 2024-07-03 11:29:57 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2024:4156 <https://access.redhat.com/errata/RHSA-2024:4156>

errata-xmlrpc 2024-07-11 11:54:28 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.14

Via RHSA-2024:4329 <https://access.redhat.com/errata/RHSA-2024:4329>

errata-xmlrpc 2024-07-17 01:37:08 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.13

Via RHSA-2024:4484 <https://access.redhat.com/errata/RHSA-2024:4484>

errata-xmlrpc 2024-08-19 05:40:42 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.12

Via RHSA-2024:5200 <https://access.redhat.com/errata/RHSA-2024:5200>

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

