

Bug 575324 (CVE-2021-34434) - Mosquitto broker with Dynamic Security Plugin may lead to access control failure

Status: CLOSED MOVED

Alias: CVE-2021-34434

Product: Community

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

Version: unspecified 

Hardware: All Linux

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

Target Milestone: --- 

Assignee: Security vulnerabilitied reported against Eclipse projects

QA Contact:


URL: <https://mosquitto.org/documentation/d...>

Whiteboard:

Keywords: security

Depends on:

Blocks:

Reported: 2021-08-09 23:25 EDT by syncxxx Song 

Modified: 2021-12-23 06:47 EST ([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.

syncxxx Song  2021-08-09 23:25:40 EDT [Description](#)

Dynamic Security Plugin is supported since Mosquitto 2.0, so this problem will affect version 2.0 and later.


Dynamic Security Plugin sets the default ACL type behaviours to:

```
* publishClientSend: deny
* publishClientReceive: allow
* subscribe: deny
* unsubscribe: allow
```


Consider the following scenario:

1. A tenant now have access to some topic like "message/state", and then he connect to broker with "cleanStart=False" and an enough "sessionInterval=10000"
2. The tenant subscribe the topic "message/state"
3. The tenant disconnect from the broker
4. Admin revoke the privilege from this tenant (subscribePattern message/state)
5. The tenant reconnect with "cleanStart=False" and his session will recover include subscription of "message/state" which means he doesn't need to send another "SUBSCRIBE" packet.
6. Because the default "publishClientReceive" is "allow", the tenant still can receive message from topic "message/state"


By the way, we can't update the default ACL with command like "mosquitto_ctrl <options> dynsec setDefaultACLAccess publishClientSend deny" when the broker is running. This could be a bug.

Wayne Beaton  2021-08-19 16:10:58 EDT [Comment 1](#)

/cc project lead


Roger Light  2021-08-22 08:59:24 EDT [Comment 2](#)

Thanks for the report, I confirm the behaviour is as you describe. I'm deciding on the best way to handle it.

Roger Light  2021-08-30 11:41:19 EDT [Comment 3](#)


Wayne, could you please assign a CVE for this please?

Versions: 2.0 to 2.0.11
CWE-285: Improper Authorization
Description: When using the dynamic security plugin, if the ability for a client to make subscriptions on a topic is revoked when a durable client is offline, then existing subscriptions for that client are not revoked.

Wayne Beaton  2021-08-30 15:31:42 EDT [Comment 4](#)

(In reply to Roger Light from [comment #3](#))
> Wayne, could you please assign a CVE for this please?

We'll use CVE-2021-34434.

Frederic Gurr  2021-12-23 06:47:59 EST [Comment 5](#)

This issue has been migrated to <https://gitlab.eclipse.org/eclipsefdn/helpdesk/-/issues/638>.