# Alpine Linux - Bug #7367

Bug # 7366 (Closed): mosquitto: Pattern based ACLs can be bypassed (CVE-2017-7650)

## [3.6] mosquitto: Pattern based ACLs can be bypassed (CVE-2017-7650)

06/01/2017 11:28 AM - Alicha CH

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 06/01/2017 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Natanael Copa | **% Done:** | 100% |
| **Category:** | Security | **Estimated time:** | 0.00 hour |
| **Target version:** | 3.6.1 | | |
| **Affected versions:** | | **Security IDs:** | |

**Description**

A vulnerability exists in Mosquitto versions 0.15 to 1.4.11.

Pattern based ACLs can be bypassed by clients that set their username/client id to '#' or '+'. This allows locally or remotely connected clients to access MQTT
topics that they do have the rights to. The same issue may be present in third party authentication/access control plugins for Mosquitto.

The vulnerability only comes into effect where pattern based ACLs are in use, or potentially where third party plugins are in use.

### Fixed In Version:

mosquitto 1.4.12

### Reference:

http://mosquitto.org/2017/05/security-advisory-cve-2017-7650/

### Patch:

https://mosquitto.org/files/cve/2017-7650/

#### Associated revisions

**Revision 79170b17 - 06/01/2017 01:03 PM - Natanael Copa**

main/mosquitto: security upgrade to 1.4.12 (CVE-2017-7650)

fixes #7367

#### History

**#1 - 06/01/2017 01:03 PM - Natanael Copa**

*- Status changed from New to Resolved*

*- % Done changed from 0 to 100*

Applied in changeset alpine:79170b170d09fe898c6c937ba588dc214dabb05c.

**#2 - 06/15/2017 10:41 AM - Alicha CH**

*- Category set to Security*

*- Status changed from Resolved to Closed*