pengwGit / **gist:d8410afeb0d5d11ab79f596a32178c2e** Secret

Last active last month

Code Revisions 4

CVE-2024-36856

gistfile1.txt

```
[CVE ID]
CVE-2024-36856
[Product]
RMQTT v0.4.0
[Problem Type]
DoS
[Description]
An issue in RMQTT v0.4.0 allows attackers to cause a Denial of Service.
[Affected Component]
Directly causing the entire broker to collapse and unable to provide normal services
[Attack Vectors]
Randomly sending a large number of malicious MQTT packets to RMQTT can cause memory resour
```

bittcrafter commented on Oct 15, 2024

Through extensive and prolonged testing, it was discovered that the rmqtt process is only killed by the operating system when memory is insufficient. This occurs because the fuzz testing tool repeatedly generates different client IDs, and in cases where there is an excessively long session expiration time.