



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

JAD Java Decompiler 1.5.8e - Local Buffer Overflow

EDB-ID:

42076

CVE:

N/A

EDB Verified: ✗

Author:

[JUAN SACCO](#)

Type:

[LOCAL](#)

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



SEARCHSPOIT MANUAL



SUBMISSIONS

```
#!/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/
#
```



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](#) >

raise

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾

 EXPLOIT DATABASE



EXPLOIT DATABASE BY OFFSEC [TERMS](#) [PRIVACY](#) [ABOUT US](#) [FAQ](#) [COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.

 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](#) >