Gallopsled / **pwntools** Public

<> Code · Issues 111 · Pull requests 43 · Discussions · Actions · Security · ...

New issue

Jump to bottom

Shellcraft generation fails with strings that contains end of multiline comment #1427

Closed **disconnect3d** opened this issue on Feb 8, 2020 · 1 comment

Labels bug shellcode

Milestone 4.2.0

disconnect3d commented on Feb 8, 2020 Contributor

PoC||GTFO:

```
In [161]: print(shellcraft.amd64.write(0, '*/', 2))
    /* write(fd=0, buf='*/', n=2) */
    /* push '*/\x00' */
    push 0x1010101 ^ 0x2f2a
    xor dword ptr [rsp], 0x1010101
    mov rsi, rsp
    xor edi, edi /* 0 */
    push 2
    pop rdx
    /* call write() */
    push SYS_write /* 1 */
    pop rax
    syscall


In [162]: asm(shellcraft.amd64.write(0, '*/', 2))
[DEBUG] cpp -C -nostdinc -undef -P -I/usr/local/lib/python2.7/dist-packages/pwnlib/data/includes /dev/stdin
[ERROR] There was an error running ['cpp', '-C', '-nostdinc', '-undef', '-P', '-I/usr/local/lib/python2.7/dist-packages/pwnlib/data/includes', '/dev/stdin']:
    It had this on stdout:
    /dev/stdin:2:27: warning: missing terminating ' character
    /dev/stdin:3:20: warning: missing terminating ' character
```

Bug is in `/* write(fd=0, buf='*/', n=2) */`, the input string ends the multi-line comment so `cpp` fails to compile our assembly.

This happens for me on `3.12.0`:

```
In [168]: pwnlib.__version__
Out[168]: '3.12.0'
```

But was also reproduced on `4.2.0dev` (commit id: `ed3c30a`).

zachriggle commented on Feb 8, 2020 Member

Good catch! I'm not sure how to handle this in a general case except
perhaps by using // comments instead?

> On Sat, Feb 8, 2020 at 5:06 PM Disconnect3d ***@***.***> wrote:
> PoC||GTFO:
>
> In [161]: print(shellcraft.amd64.write(0, '*/', 2))
>   /* write(fd=0, buf='*/', n=2) */
>   /* push '*/\x00' */
>   push 0x1010101 ^ 0x2f2a
>   xor dword ptr [rsp], 0x1010101
>   mov rsi, rsp
>   xor edi, edi /* 0 */
>   push 2
>   pop rdx
>   /* call write() */
>   push SYS_write /* 1 */
>   pop rax
>   syscall
>
>
> In [162]: asm(shellcraft.amd64.write(0, '*/', 2))
> [DEBUG] cpp -C -nostdinc -undef -P -I/usr/local/lib/python2.7/dist-packages/pwnlib/data/includes /dev/stdin
> [ERROR] There was an error running ['cpp', '-C', '-nostdinc', '-undef', '-P', '-I/usr/local/lib/python2.7/dist-packages/pwnlib/data/includes', '/dev/stdin']:
>   It had this on stdout:
>   /dev/stdin:2:27: warning: missing terminating ' character
>   /dev/stdin:3:20: warning: missing terminating ' character
>
> Bug is in /* write(fd=0, buf='*/', n=2) */, the input string ends the
> multi-line comment so cpp fails to compile our assembly.
>
> This happens for me on 3.12.0:
>
> In [168]: pwnlib.__version__
> Out[168]: '3.12.0'
>
> But was also reproduced on 4.2.0dev (commit id: `ed3c30a`
> < `ed3c30a` >

>).
>
> —
> You are receiving this because you are subscribed to this thread.
> Reply to this email directly, view it on GitHub
> <#1427?
> email_source=notifications&email_token=AAA3IGD3O2TYLWOINVUWZNLRB43I5A5CNFSM4KR5TGU2YY3PNVWWK3TUL52HS4DFUVEXG43VMWVGG33NNVSW45C7NFSM4IMA2YAQ>,
> or unsubscribe
> <https://github.com/notifications/unsubscribe-auth/AAA3IGCF6ZRQOXXW6PFTE33RB43I5ANCNFSM4KR5TGUQ>
> .

--

Zach Riggle

Arusekk added the **shellcode** label on Feb 9, 2020

Arusekk added the bug label on Apr 23, 2020

Arusekk added this to the **4.2.0** milestone on Jun 3, 2020

Arusekk mentioned this issue on Nov 29, 2020

Fix pwntools shellcraft SSTI vulnerability #1732

Merged

Arusekk closed this as completed in `138188e` on Nov 29, 2020

Assignees

No one assigned

Labels

bug shellcode

Projects

None yet

Milestone

4.2.0

Development

No branches or pull requests

3 participants