New issue

Jump to bottom

Could not supply a percent symbol for webcontrol param update #1227

Closed **tosiara** opened this issue on Oct 20, 2020 · 11 comments · Fixed by #1232

Labels bug

tosiara commented on Oct 20, 2020 Member

There is no way to put a percent symbol as param value, for example, `text_left` :

```
$ curl http://localhost:8080/1/config/set?text_left=%
<!DOCTYPE html>
<html>
<body>
<p>Bad Request</p>
<p>The server did not understand your request.</p>
</body>
</html>
```

https://sourceforge.net/p/motion/mailman/message/37127567/

tosiara added the bug label on Oct 20, 2020

tosiara commented on Oct 20, 2020 Member Author

There is also segfault with a string `%a` :

```
curl http://localhost:8080/1/config/set?text_left=%a

[0:cn0] [DBG] [STR] webu_parseurl: Sent url: /1/config/set?text_left=%a
Segmentation fault
```

tosiara commented on Oct 20, 2020 Member Author

```
[New Thread 0x437ff460 (LWP 24533)]
[0:cn0] [DBG] [STR] webu_parseurl: Sent url: /1/config/set?text_left=%a
*** Error in `/home/motion/git/motion/src/motion': realloc(): invalid next size: 0x43804d20 ***

Program received signal SIGABRT, Aborted.
[Switching to Thread 0x437ff460 (LWP 24533)]
__libc_do_syscall () at ../ports/sysdeps/unix/sysv/linux/arm/libc-do-syscall.S:44
44      ../ports/sysdeps/unix/sysv/linux/arm/libc-do-syscall.S: No such file or directory.
(gdb) bt
#0  __libc_do_syscall () at ../ports/sysdeps/unix/sysv/linux/arm/libc-do-syscall.S:44
#1  0x40224ebe in __GI_raise (sig=sig@entry=6) at ../nptl/sysdeps/unix/sysv/linux/raise.c:56
#2  0x40227716 in __GI_abort () at abort.c:89
#3  0x4024b12c in __libc_message (do_abort=<optimized out>, fmt=0x402ce114 "*** Error in `%s': %s: 0x%s ***\n") at ../sysdeps/posix/libc_fatal.c:175
#4  0x40251c7e in malloc_printerr (action=1, str=0x402cea8c "realloc(): invalid next size", ptr=<optimized out>) at malloc.c:4998
#5  0x4025433a in _int_realloc (av=av@entry=0x43800010, oldp=oldp@entry=0x43804d18, oldsize=oldsize@entry=8200, nb=nb@entry=88) at malloc.c:4236
#6  0x40255178 in __GI___libc_realloc (oldmem=0x43804d20, bytes=84) at malloc.c:3031
#7  0x4024a10c in _IO_mem_finish (fp=0x43804ba0, dummy=<optimized out>) at memstream.c:134
#8  0x402470ac in _IO_new_fclose (fp=fp@entry=0x43804ba0) at iofclose.c:63
#9  0x40291368 in __GI___vsyslog_chk (pri=<optimized out>, flag=1, fmt=fmt@entry=0x7e4c4c "%s", ap=ap@entry=...) at ../misc/syslog.c:226
#10 0x40291684 in __syslog_chk (pri=<optimized out>, flag=<optimized out>, fmt=0x7e4c4c "%s") at ../misc/syslog.c:129
#11 0x0006c424 in motion_log ()
#12 0x00089af4 in webu_parseurl ()
#13 0x0008a04a in webu_mhd_init ()
#14 0x40064b92 in ?? () from /usr/lib/arm-linux-gnueabihf/libmicrohttpd.so.10
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
```

d0td0tslash commented on Oct 24, 2020

Hello **@tosiara**,
This issue was privately submitted to **@Mr-DaveDev** on October 5th 2020 due to its sensitive nature (Denial of Service Condition).

The issue here is not about the `%` itself, it's about how data is parsed within the web server.
e.g. `%2F` is a valid URL encoded string that is translated to `/` within a request.

The problem lays on the `web_url_decode()` function in web.c which expects an hex value (2 chars) after a `%` is passed in a request however, if only one character is passed, the while loop here will continue looking for *data in a memory section that shouldn't be readable, causing an Out of Bound Heap Read condition (that will ultimately result in segfault).

Below, a more detailed dump using `-fsanitize=address` and `-DDEBUG` flags:

```
Reading symbols from ./motion...
(gdb) r
Starting program: /root/motion/src/motion
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/i386-linux-gnu/libthread_db.so.1".
[0:motion] [NTC] [ALL] conf_load: Processing thread 0 - config file /root/motion/src/motion.conf
[0:motion] [NTC] [ALL] motion_startup: Logging to syslog
```

```
[New Thread 0xa5dfeb40 (LWP 17903)]
[New Thread 0xa4dffb40 (LWP 17904)]
[New Thread 0xa2603b40 (LWP 17905)]
=================================================================
==17898==ERROR: AddressSanitizer: heap-buffer-overflow on address 0xa8a07d00 at pc 0x0049354b bp 0xa2602428 sp 0xa260241c
READ of size 1 at 0xa8a07d00 thread T4 (cn0)
    0 0x49354a in webu_url_decode /root/motion/src/webu.c:254
    1 0x49354a in webu_parseurl /root/motion/src/webu.c:480
    2 0x49430b in webu_mhd_init /root/motion/src/webu.c:1405
    3 0xb7966d0d  (/lib/i386-linux-gnu/libmicrohttpd.so.12+0x7d0d)
    4 0xb7967f9c  (/lib/i386-linux-gnu/libmicrohttpd.so.12+0x8f9c)
    5 0xb796b195  (/lib/i386-linux-gnu/libmicrohttpd.so.12+0xc195)
    6 0xb7a643ce  (/lib/i386-linux-gnu/libasan.so.6+0x513ce)
    7 0xb5d170b3 in start_thread nptl/pthread_create.c:477
    8 0xb5c2a2c5 in __clone (/lib/i386-linux-gnu/libc.so.6+0x1042c5)
0xa8a07d00 is located 0 bytes to the right of 512-byte region [0xa8a07b00,0xa8a07d00)
allocated by thread T4 (cn0) here:
    0 0xb7abf673 in __interceptor_calloc (/lib/i386-linux-gnu/libasan.so.6+0xac673)
    1 0x41a35b in mymalloc /root/motion/src/motion.c:3690
Thread T4 (cn0) created by T2 (MHD-listen) here:
    0 0xb7a64440 in pthread_create (/lib/i386-linux-gnu/libasan.so.6+0x51440)
    1 0xb79724f1  (/lib/i386-linux-gnu/libmicrohttpd.so.12+0x134f1)
Thread T2 (MHD-listen) created by T0 here:
    0 0xb7a64440 in pthread_create (/lib/i386-linux-gnu/libasan.so.6+0x51440)
    1 0xb79724f1  (/lib/i386-linux-gnu/libmicrohttpd.so.12+0x134f1)
SUMMARY: AddressSanitizer: heap-buffer-overflow /root/motion/src/webu.c:254 in webu_url_decode
Shadow bytes around the buggy address:
  0x35140f50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x35140f60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x35140f70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x35140f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x35140f90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x35140fa0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x35140fb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x35140fc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x35140fd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x35140fe0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x35140ff0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==17898==ABORTING
[Thread 0xa4dffb40 (LWP 17904) exited]
[Thread 0xa5dfeb40 (LWP 17903) exited]
[Thread 0xa65ffb40 (LWP 17902) exited]
[Thread 0xab57f080 (LWP 17898) exited]
[Inferior 1 (process 17898) exited with code 01]
```

This can happen in any part of the URL (also from an unauthenticated perspective), not only the `/1/config/set?text_left=` parameter.

Proof of concept:

```
GET
/%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%A%00
HTTP/1.1
Host: 192.168.126.128:8080
Connection: close
```

Unfortunately, after the segfault has happened, a manual intervention to re-run the motion service is required.
This issue received the following Common Vulnerabilities and Exposures number `CVE-2020-26566` on the 5th of October 2020.

tosiara commented on Oct 24, 2020 Member Author

Have you also checked if the stream url parsing also affected (on port 8081)?
And did MrDave respond to you about estimated time to fix?

tosiara commented on Oct 24, 2020 • edited

Member Author

Oh, I have just checked and the stream url also segfaults. This would have higher risk as users tend to expose the stream port

d0td0tslash commented on Oct 24, 2020

> Have you also checked if the stream url parsing also affected (on port 8081)?
> And did MrDave respond to you about estimated time to fix?

> Oh, I have just checked and the stream url also segfaults. This would have higher risk as users tend to expose the stream port

Yes, unfortunately this also affects the stream port.

Mr-DaveDev mentioned this issue on Oct 25, 2020

Use MHD functions for url decoding #1232

Merged

Mr-DaveDev commented on Oct 25, 2020 Contributor

I believe that PR #1232 will resolve this.

Can someone validate?

tosiara commented on Oct 25, 2020 Member Author

I have checked the PR, the issue seems resolved

Before the fix:

```
$ curl http://localhost:8080/%a
<!DOCTYPE html>
<html>
<body>
<p>Bad Request</p>
<p>The server did not understand your request.</p>
</body>
</html>
```

```
[0:cn0] [ERR] [STR] webu_url_decode: Error decoding url
free(): invalid pointer
Aborted (core dumped)
```

```
$ curl http://localhost:8081/%a
<!DOCTYPE html>
<html>
<body>
<p>Bad Request</p>
<p>The server did not understand your request.</p>
</body>
</html>
```

```
[0:cn0] [ERR] [STR] webu_url_decode: Error decoding url
free(): invalid pointer
Aborted (core dumped)
```

After the fix:

```
$ curl http://localhost:8080/%a
<!DOCTYPE html>
<html>
<body>
<p>Bad Request</p>
<p>The server did not understand your request.</p>
</body>
</html>

[0:wu0] [INF] [ALL] webu_clientip: Connection from: 127.0.0.1
[0:wu0] [INF] [STR] webu_html_main: Invalid action requested: >%a< >< ><
```

```
$ curl http://localhost:8081/%a
<html><head><title>Access denied</title></head><body>Access denied</body></html>

[0:st0] [INF] [ALL] webu_clientip: Connection from: 127.0.0.1
```

Ubuntu 14 build break:

```
src/webu.c:414: undefined reference to `MHD_http_unescape'
```

Mr-Dave closed this as completed in #1232 on Oct 25, 2020

tosiara commented on Oct 25, 2020 • edited Member Author

@Mr-Dave could you also create a tag, ex `4.3.2` or anything, and make a release?
I could then kick off my build machine and build debs for that release, as well as post an announcement and encourage users to update

tosiara commented on Oct 25, 2020 Member Author

Or, we could merge the fix into 4.3, as master has many changes including param rename. So just updating 4.3 bracnh would be more convenient to users to update

- ☑ Created Github security advisory draft to activate dependency bot.
- ☑ Pepared a draft for mail list.
- ☑ Builds are running and should be ready in an hour.
- ☑ Full disclosure

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Use MHD functions for url decoding
Mr-DaveDev/motion

3 participants