

New issue

[Jump to bottom](#)

heap-use-after-free in ecma_bytecode_ref #4056

🔒 Closed owl337 opened this issue on Jul 25, 2020 · 0 comments · Fixed by #4068

Assignees



Labels

bug

owl337 commented on Jul 25, 2020

JerryScript revision

[da5b058](#)

Build platform

Ubuntu 16.04.6 LTS (Linux 4.15.0-99-generic x86_64)

Build steps

```
./tools/build.py --clean --debug --compile-flag=-fsanitize=address \
--compile-flag=-m32 --compile-flag=-fno-omit-frame-pointer \
--compile-flag=-fno-common --compile-flag=-g --strip=off \
--system-allocator=on --logging=on --linker-flag=-fuse-ld=gold \
--error-messages=on --profile=es2015-subset --lto=off
```

Test case

```
function echo(RegExp) {
  try { (r).compile(r).compile(RegExp.prototype) } catch (err) { }
}

var suppressLastIndex = false;
var suppressRegExp = false;
var suppressIndex = false;

function safeCall(f) {
  var args = [];
  for (var a = 1; a < arguments.length; ++a)
    args.push(arguments[a]);
  try {
    return f.apply(this, args);
  } catch (ex) {
    echo("EXCEPTION");
  }
}

function dump(o) {
  var sb = [];
  if (o === null)
    sb.push("null");
  else if (o === undefined)
    sb.push("undefined");
  else if (o === true)
    sb.push("true");
  else if (o === false)
    sb.push("false");
  else if (typeof o === "number")
    sb.push(o.toString());
  else if (typeof o === "string") {
    if (o.length > 8192)
      sb.push("<long string>");
    else {
      sb.push("");
      var start = -1;
      for (var i = 0; i < o.length; i++) {
        var c = o.charCodeAt(i);
        if (c < 32 || c > 127 || c === '''.charCodeAt(0) || c === '\\'.charCodeAt(0)) {
          if (start >= 0)
            sb.push(o.substring(start, i));
          start = -1;
          sb.push("\\u");
          sb.push(String.fromCharCode(hex.charCodeAt((c >> 12) & 0xf)));
          sb.push(String.fromCharCode(hex.charCodeAt((c >> 8) & 0xf)));
          sb.push(String.fromCharCode(hex.charCodeAt((c >> 4) & 0xf)));
          sb.push(String.fromCharCode(hex.charCodeAt((c >> 0) & 0xf)));
        }
        else {
          if (start < 0)
            start = i;
        }
      }
      if (start >= 0)
        sb.push(o.substring(start, o.length));
      sb.push("");
    }
  }
}

else if (o instanceof RegExp) {
  var body = o.source;
  sb.push("/");
  var start = -1;
  for (var i = 0; i < body.length; i++) {
    var c = body.charCodeAt(i);
```

```

        if (c < 32 || c > 127) {
            if (start >= 0)
                sb.push(body.substring(start, i));
            start = -1;
            sb.push("\\u");
            sb.push(String.fromCharCode(hex.charCodeAt((c >> 12) & 0xf)));
            sb.push(String.fromCharCode(hex.charCodeAt((c >> 8) & 0xf)));
            sb.push(String.fromCharCode(hex.charCodeAt((c >> 4) & 0xf)));
            sb.push(String.fromCharCode(hex.charCodeAt((c >> 0) & 0xf)));
        }
        else {
            if (start < 0)
                start = i;
        }
    }
    if (start >= 0)
        sb.push(body.substring(start, body.length));
    sb.push("/");
    if (o.global)
        sb.push("g");
    if (o.ignoreCase)
        sb.push("i");
    if (o.multiline)
        sb.push("m");
    if (!suppressLastIndex && o.lastIndex !== undefined) {
        sb.push(" /*lastIndex=");
        sb.push(o.lastIndex);
        sb.push("/ ");
    }
}
else if (o.length !== undefined) {
    sb.push("[");
    for (var i = 0; i < o.length; i++) {
        if (i > 0)
            sb.push(",");
        sb.push(dump(o[i]));
    }
    sb.push("]");
    if (!suppressIndex && (o.input !== undefined || o.index !== undefined))
    {
        sb.push(" /*input=");
        sb.push(dump(o.input));
        sb.push(", index=");
        sb.push(dump(o.index));
        sb.push("/ ");
    }
}
else if (o.toString !== undefined) {
    sb.push("<object with toString>");
}
else
    sb.push(o.toString());
return sb.join("");
}

function pre(w, origargs, n) {
    var sb = [];
    sb.push("(");
    for (var i = 0; i < n; i++) {
        if (i > 0) sb.push(", ");
        sb.push(dump(origargs[i]));
    }
    if (origargs.length > n) {
        sb.push(", ");
        sb.push(dump(origargs[n]));
        origargs[0].lastIndex = origargs[n];
    }
    sb.push(")");
    echo(sb.join(""));
}

function post(r) {
    if (!suppressLastIndex) {
        echo("r.lastIndex=" + dump(r.lastIndex));
    }
    if (!suppressRegExp) {
        var sb = [];
        sb.push("RegExp. ${_,1,...,9}=[");
        sb.push(dump(RegExp.$_));
        for (var i = 1; i <= 9; i++) {
            sb.push(",");
            sb.push(dump(RegExp["$" + i]));
        }
        sb.push("]");
        echo(sb.join(""));
    }
}

function exec(r, s) {
    pre("exec", arguments, 2);
    echo(dump(r.exec(s)));
    post(r);
}

function test(r, s) {
    pre("test", arguments, 2);
    echo(dump(r.test(s)));
    post(r);
}

function replace(r, s, o) {
    pre("replace", arguments, 3);
    echo(dump(s.replace(r, o)));
    post(r);
}

function split(r, s) {
    pre("split", arguments, 2);
    echo(dump(s.split(r)));
    post(r);
}

function match(r, s) {

```

```

    pre("match", arguments, 2);
    echo(dump(s.match(r)));
    post(r);
}

function search(r, s) {
    pre("search", arguments, 2);
    echo(dump(s.search(r)));
    post(r);
}

function bogus(r, o) {
    echo("bogus(" + dump(r) + ", " + dump(o) + ")");
    try { new RegExp(r, o); echo("FAILED"); } catch (e) { echo("PASSED"); }
}

var r, s;
r = /a*/g;
s = "cdsdddfs";
exec(r, s);
exec(r, s);

```

Output

```

=====
==80830==ERROR: AddressSanitizer: heap-use-after-free on address 0xf6502022 at pc 0x08073345 bp 0xffe00ad8 sp 0xffe00ac8
READ of size 2 at 0xf6502022 thread T0
#0 0x8073344 in ecma_bytecode_ref /home/jerryscript/jerry-core/ecma/base/ecma-helpers.c:1344
#1 0x80b41fb in ecma_op_create_regexp_from_bytecode /home/jerryscript/jerry-core/ecma/operations/ecma-regexp-object.c:362
#2 0x8133fe1 in ecma_builtin_regexp_prototype_compile /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp-prototype.c:320
#3 0x813455b in ecma_builtin_regexp_prototype_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp-prototype.c:567
#4 0x808281d in ecma_builtin_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1216
#5 0x80829c3 in ecma_builtin_dispatch_call /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1240
#6 0x8098e38 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:845
#7 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#8 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#9 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#10 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#11 0x8099320 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:943
#12 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#13 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#14 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#15 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#16 0x8099320 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:943
#17 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#18 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#19 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#20 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#21 0x8099320 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:943
#22 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#23 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#24 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#25 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#26 0x80f9aff in vm_run_global /home/jerryscript/jerry-core/vm/vm.c:339
#27 0x804def4 in jerry_run /home/jerryscript/jerry-core/api/jerry.c:579
#28 0x804acbf in main /home/jerryscript/jerry-main/main-unix.c:759
#29 0xf788646 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18646)
#30 0x8048fb0 (/home/jerryscript/build/bin/jerry+0x8048fb0)

0xf6502022 is located 2 bytes inside of 24-byte region [0xf6502020,0xf6502038)
freed by thread T0 here:
#0 0xf7abdb84 in free (/usr/lib32/libasan.so.2+0x96a84)
#1 0x80c2885 in jmem_heap_free_block_internal /home/jerryscript/jerry-core/jmem/jmem-heap.c:476
#2 0x80c2c1d in jmem_heap_free_block /home/jerryscript/jerry-core/jmem/jmem-heap.c:685
#3 0x80738ff in ecma_bytecode_deref /home/jerryscript/jerry-core/ecma/base/ecma-helpers.c:1467
#4 0x8133fd0 in ecma_builtin_regexp_prototype_compile /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp-prototype.c:319
#5 0x813455b in ecma_builtin_regexp_prototype_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp-prototype.c:567
#6 0x808281d in ecma_builtin_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1216
#7 0x80829c3 in ecma_builtin_dispatch_call /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1240
#8 0x8098e38 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:845
#9 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#10 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#11 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#12 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#13 0x8099320 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:943
#14 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#15 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#16 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#17 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#18 0x8099320 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:943
#19 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#20 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#21 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#22 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#23 0x8099320 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:943
#24 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#25 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#26 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#27 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#28 0x80f9aff in vm_run_global /home/jerryscript/jerry-core/vm/vm.c:339
#29 0x804def4 in jerry_run /home/jerryscript/jerry-core/api/jerry.c:579

previously allocated by thread T0 here:
#0 0xf7abe144 in __interceptor_realloc (/usr/lib32/libasan.so.2+0x97144)
#1 0x80c2bfe in jmem_heap_realloc_block /home/jerryscript/jerry-core/jmem/jmem-heap.c:674
#2 0x80eb507 in re_compile_bytecode /home/jerryscript/jerry-core/parser/regexp/re-compiler.c:144
#3 0x80b412e in ecma_op_create_regexp_from_pattern /home/jerryscript/jerry-core/ecma/operations/ecma-regexp-object.c:336
#4 0x8133f77 in ecma_builtin_regexp_prototype_compile /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp-prototype.c:323
#5 0x813455b in ecma_builtin_regexp_prototype_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp-prototype.c:567
#6 0x808281d in ecma_builtin_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1216
#7 0x80829c3 in ecma_builtin_dispatch_call /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1240
#8 0x8098e38 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:845
#9 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#10 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#11 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#12 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#13 0x8099320 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:943
#14 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#15 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778

```

```
#16 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#17 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#18 0x8099320 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:943
#19 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#20 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#21 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#22 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#23 0x8099320 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:943
#24 0x8099c3f in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1142
#25 0x80fb2f7 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:778
#26 0x810e095 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4690
#27 0x810e5d9 in vm_run /home/jerryscript/jerry-core/vm/vm.c:4792
#28 0x80f9aff in vm_run_global /home/jerryscript/jerry-core/vm/vm.c:339
#29 0x804def4 in jerry_run /home/jerryscript/jerry-core/api/jerry.c:579

SUMMARY: AddressSanitizer: heap-use-after-free /home/jerryscript/jerry-core/ecma/base/ecma-helpers.c:1344 ecma_bytecode_ref
Shadow bytes around the buggy address:
 0x3eca03b0: fd fd fd fd fa fa fd fd fd fa fa fd fd fd fd
 0x3eca03c0: fa fa fd fd fd fa fa fd fd fd fa fa fd fd fd
 0x3eca03d0: fd fd fa fa fd fd fd fa fa fd fd fd fa fa
 0x3eca03e0: fd fd fd fa fa fd fd fd fd fa fa fd fd fd fa
 0x3eca03f0: fa fa fd fd fd fa fa fd fd fd fa fa 00 00
=>0x3eca0400: 00 fa fa fa[fd]fd fd fa fa fd fd fd fa fa
 0x3eca0410: fd fd fd fa fa 00 00 00 fa fa 00 00 00 fa
 0x3eca0420: fa fa fd fd fd fa fa fd fd fd fa fa fd fd
 0x3eca0430: fd fd fa fa fd fd fd fd fa fa fd fd fd fa fa
 0x3eca0440: fd fd fd fa fa fd fd fd fa fa fd fd fd fd
 0x3eca0450: fa fa fd fd fd fa fa fd fd fd fa fa fd fd
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
Heap right redzone: fb
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack partial redzone: f4
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
==80830==ABORTING
```

Credits: This vulnerability is detected by chong from OWL337.

 rerobika assigned dbatyai on Jul 27, 2020

 rerobika added the bug label on Jul 27, 2020

 dbatyai pushed a commit to dbatyai/jerryscript that referenced this issue on Jul 27, 2020

Fix a use-after-free in RegExp.prototype.compile ...

✗ f8b2c39

 dbatyai pushed a commit to dbatyai/jerryscript that referenced this issue on Jul 27, 2020

Fix a use-after-free in RegExp.prototype.compile ...

✗ 7918488

 dbatyai pushed a commit to dbatyai/jerryscript that referenced this issue on Jul 27, 2020

Fix a use-after-free in RegExp.prototype.compile ...

✓ bf2c9e1

 dbatyai mentioned this issue on Jul 27, 2020

Fix a use-after-free in RegExp.prototype.compile #4068

 Merged

 LaszloLango closed this as completed in #4068 on Jul 28, 2020

 LaszloLango pushed a commit that referenced this issue on Jul 28, 2020

Fix a use-after-free in RegExp.prototype.compile (#4068) ...

✓ 20f83d9

Assignees

 dbatyai

Labels

bug

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fix a use-after-free in RegExp.prototype.compile**
dbatyai/jerryscript

3 participants

