Starred by 4 users

Owner:	pthier@chromium.org
CC:	leszeks@chromium.org pthier@chromium.org anapesko@google.com vahl@chromium.org jgruber@chromium.org mathias@chromium.org verwa...@chromium.org ishell@chromium.org ecmziegler@google.com
Status:	Verified *(Closed)*
Components:	Blink>JavaScript>Runtime Blink>JavaScript>Regexp
Modified:	Jun 23, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2021-01-20
OS:	Linux, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-5000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
ClusterFuzz-Verified
Test-Predator-Auto-Components
CVE_description-submitted
M-89
Target-89
FoundIn-87
FoundIn-88
merge-merged-8.6
LTR-Merged-86
LTS-Security-86
Release-0-M89
external_security_report
merge-merged-8.9

Issue 1166138: Security: Debug check failed: kMinCPOffset <= by (-32768 vs. -65536).

Reported by p4nda...@gmail.com on Wed, Jan 13, 2021, 6:51 AM EST

Code

VULNERABILITY DETAILS

In ChoiceNode::Emit, we can control text_length via regexp object.

```c++
void ChoiceNode::Emit(RegExpCompiler* compiler, Trace* trace) {
  int choice_count = alternatives_->length();

  if (choice_count == 1 && alternatives_->at(0).guards() == nullptr) {
    alternatives_->at(0).node()->Emit(compiler, trace);
    return;
  }

  AssertGuardsMentionRegisters(trace);

  LimitResult limit_result = LimitVersions(compiler, trace);
  if (limit_result == DONE) return;
  DCHECK(limit_result == CONTINUE);

  // For loop nodes we already flushed (see LoopChoiceNode::Emit), but for
  // other choice nodes we only flush if we are out of code size budget.
  if (trace->flush_budget() == 0 && trace->actions() != nullptr) {
    trace->Flush(compiler, this);
    return;
  }

  RecursionCheck rc(compiler);

  PreloadState preload;
  preload.init();
  GreedyLoopState greedy_loop_state(not_at_start());

 [1]  int text_length = GreedyLoopTextLengthForAlternative(&alternatives_->at(0));
  AlternativeGenerationList alt_gens(choice_count, zone());

  if (choice_count > 1 && text_length != kNodeIsTooComplexForGreedyLoops) {
 [2]   trace = EmitGreedyLoop(compiler, trace, &alt_gens, &preload,
                               &greedy_loop_state, text_length);
  } else {
      // ...
  }
    //...
}
```

So when calling EmitGreedyLoop, it'll fail at 'DCHECK_LE(kMinCPOffset, by)' in RegExpBytecodeGenerator::AdvanceCurrentPosition. and then set advance_current_offset_

as the text_length.
```c++
void RegExpBytecodeGenerator::AdvanceCurrentPosition(int by) {
  DCHECK_LE(kMinCPOffset, by); //
  DCHECK_GE(kMaxCPOffset, by);
  advance_current_start_ = pc_;
  advance_current_offset_ = by;
  Emit(BC_ADVANCE_CP, by);
  advance_current_end_ = pc_;
}

```

VERSION
v8 Version: commit cbed65f4f55628304c002886db425f5e342f6b18
Operating System: Ubuntu 20.04 64bit

REPRODUCTION CASE
1. execute the attach file with d8 debug version.
2. in debug version, it will crash at the assert in vector access as below:

```
#
# Fatal error in ../../src/objects/js-locale.cc, line 408
# Debug check failed: U_SUCCESS(status).
#
#
#
#FailureMessage Object: 0x7ffe6d7ed040
==== C stack trace ===============================

    /home/p4nda/v8/out.gn/x64.debug/libv8_libbase.so(v8::base::debug::StackTrace::StackTrace()+0x1e) [0x7fc085b53d2e]
    /home/p4nda/v8/out.gn/x64.debug/libv8_libplatform.so(+0x5939d) [0x7fc085ad139d]
    /home/p4nda/v8/out.gn/x64.debug/libv8_libbase.so(V8_Fatal(char const*, int, char const*, ...)+0x230) [0x7fc085b383e0]
    /home/p4nda/v8/out.gn/x64.debug/libv8_libbase.so(+0x40dac) [0x7fc085b37dac]
    /home/p4nda/v8/out.gn/x64.debug/libv8_libbase.so(V8_Dcheck(char const*, int, char const*)+0x27) [0x7fc085b38497]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::JSLocale::Minimize(v8::internal::Isolate*, v8::internal::Handle<v8::internal::JSLocale>)+0xe7) [0x7fc0886e3a07]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(+0x23d95ba) [0x7fc087f385ba]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::Builtin_LocalePrototypeMinimize(int, unsigned long*, v8::internal::Isolate*)+0xf8) [0x7fc087f381d8]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(+0x1d215bf) [0x7fc0878805bf]
Received signal 4 ILL_ILLOPN 7fc085b50ee1
[2]    3320345 illegal hardware instruction (core dumped)  ~/v8/out.gn/x64.debug/d8 --allow-natives-syntax
```

test.js
90 bytes View Download

Comment 1 by p4nda...@gmail.com on Wed, Jan 13, 2021, 6:54 AM EST
the crash log is below:

```
#
# Fatal error in ../../src/regexp/regexp-bytecode-generator.cc, line 168
# Debug check failed: kMinCPOffset <= by (-32768 vs. -65536).
#
#
#
#FailureMessage Object: 0x7ffeb8f23e40
==== C stack trace ===============================

    /home/p4nda/v8/out.gn/x64.debug/libv8_libbase.so(v8::base::debug::StackTrace::StackTrace()+0x1e) [0x7fe385e2fd2e]
    /home/p4nda/v8/out.gn/x64.debug/libv8_libplatform.so(+0x5939d) [0x7fe385dad39d]
    /home/p4nda/v8/out.gn/x64.debug/libv8_libbase.so(V8_Fatal(char const*, int, char const*, ...)+0x230) [0x7fe385e143e0]
    /home/p4nda/v8/out.gn/x64.debug/libv8_libbase.so(+0x40dac) [0x7fe385e13dac]
    /home/p4nda/v8/out.gn/x64.debug/libv8_libbase.so(V8_Dcheck(char const*, int, char const*)+0x27) [0x7fe385e14497]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::RegExpBytecodeGenerator::AdvanceCurrentPosition(int)+0x65) [0x7fe388c89155]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::ChoiceNode::EmitGreedyLoop(v8::internal::RegExpCompiler*, v8::internal::Trace*,
v8::internal::AlternativeGenerationList*, v8::internal::PreloadState*, v8::internal::GreedyLoopState*, int)+0x25a) [0x7fe388cb521a]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::ChoiceNode::Emit(v8::internal::RegExpCompiler*, v8::internal::Trace*)+0x26d) [0x7fe388cb38fd]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::LoopChoiceNode::Emit(v8::internal::RegExpCompiler*, v8::internal::Trace*)+0x1e9) [0x7fe388cb3689]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::Trace::Flush(v8::internal::RegExpCompiler*, v8::internal::RegExpNode*)+0x2c0) [0x7fe388cac7f0]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::LoopChoiceNode::Emit(v8::internal::RegExpCompiler*, v8::internal::Trace*)+0x1d3) [0x7fe388cb3673]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::ActionNode::Emit(v8::internal::RegExpCompiler*, v8::internal::Trace*)+0x198) [0x7fe388cb5ed8]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::RegExpCompiler::Assemble(v8::internal::Isolate*, v8::internal::RegExpMacroAssembler*,
v8::internal::RegExpNode*, int, v8::internal::Handle<v8::internal::String>)+0x1b0) [0x7fe388cab8d0]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::RegExpImpl::Compile(v8::internal::Isolate*, v8::internal::Zone*, v8::internal::RegExpCompileData*,
v8::base::Flags<v8::internal::JSRegExp::Flag, int>, v8::internal::Handle<v8::internal::String>, v8::internal::Handle<v8::internal::String>, bool, unsigned int&)+0x822)
[0x7fe388cf1502]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::RegExpImpl::CompileIrregexp(v8::internal::Isolate*, v8::internal::Handle<v8::internal::JSRegExp>,
v8::internal::Handle<v8::internal::String>, bool)+0x3c0) [0x7fe388cf0390]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::RegExpImpl::EnsureCompiledIrregexp(v8::internal::Isolate*, v8::internal::Handle<v8::internal::JSRegExp>,
v8::internal::Handle<v8::internal::String>, bool)+0x2a8) [0x7fe388cf41e8]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::RegExpImpl::IrregexpPrepare(v8::internal::Isolate*, v8::internal::Handle<v8::internal::JSRegExp>,
v8::internal::Handle<v8::internal::String>)+0xaa) [0x7fe388ceecfa]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::RegExpImpl::IrregexpExec(v8::internal::Isolate*, v8::internal::Handle<v8::internal::JSRegExp>,
v8::internal::Handle<v8::internal::String>, int, v8::internal::Handle<v8::internal::RegExpMatchInfo>)+0x2c7) [0x7fe388cef3c7]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::RegExp::Exec(v8::internal::Isolate*, v8::internal::Handle<v8::internal::JSRegExp>,
v8::internal::Handle<v8::internal::String>, int, v8::internal::Handle<v8::internal::RegExpMatchInfo>)+0xf5) [0x7fe388ceee95]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(+0x2f53298) [0x7fe388d8e298]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(v8::internal::Runtime_RegExpExec(int, unsigned long*, v8::internal::Isolate*)+0x11d) [0x7fe388d8dbfd]
    /home/p4nda/v8/out.gn/x64.debug/libv8.so(+0x1d2149f) [0x7fe387b5c49f]
Received signal 4 ILL_ILLOPN 7fe385e2cee1
[2]    2705996 illegal hardware instruction (core dumped)  ~/v8/out.gn/x64.debug/d8 --allow-natives-syntax ./test.js
```

Comment 2 by sheriffbot on Wed, Jan 13, 2021, 6:56 AM EST Project Member

Labels: reward-potential

Comment 3 by ClusterFuzz on Wed, Jan 13, 2021, 7:35 AM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5752813136445440.

Comment 4 by ClusterFuzz on Wed, Jan 13, 2021, 7:56 AM EST Project Member

Labels: OS-Linux

Comment 5 by ClusterFuzz on Wed, Jan 13, 2021, 8:03 AM EST Project Member

Labels: OS-Mac

Comment 6 by jgruber@chromium.org on Wed, Jan 13, 2021, 8:14 AM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: jgruber@chromium.org
Cc: pthier@chromium.org

Thanks, I can reproduce. It's possible to overflow the 24 bits for the offset in the ADVANCE_CP bytecode and thus trick the regexp interpreter to advance to an incorrect offset. Let's turn these into runtime checks first before looking into the underlying issue.

Comment 7 by jgruber@chromium.org on Wed, Jan 13, 2021, 8:16 AM EST Project Member

Labels: Pri-1

I'm assuming an OOB read is possible by turning the negative offset into a positive offset.

Comment 8 by ClusterFuzz on Wed, Jan 13, 2021, 8:16 AM EST Project Member

Labels: FoundIn-88 FoundIn-87 Security_Impact-Stable

Detailed Report: https://clusterfuzz.com/testcase?key=5752813136445440

Fuzzer: None
Job Type: linux_asan_d8_dbg
Platform Id: linux

Crash Type: DCHECK failure
Crash Address:
Crash State:
  kMinCPOffset <= by in regexp-bytecode-generator.cc
  v8::internal::RegExpBytecodeGenerator::AdvanceCurrentPosition
  v8::internal::ChoiceNode::EmitGreedyLoop

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_d8_dbg&range=63904:63905

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5752813136445440

The reproduce tool requires a ClusterFuzz source checkout. To prepare one, run:

git clone https://github.com/google/clusterfuzz && cd clusterfuzz && git checkout tags/reproduce-tool-stable

To reproduce this issue, run:

./reproduce.sh -t https://clusterfuzz.com/testcase-detail/5752813136445440 -b /path/to/build

Please use the GN arguments provided in this report when building the binary. If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 9 by ClusterFuzz on Wed, Jan 13, 2021, 8:23 AM EST Project Member

Labels: Test-Predator-Auto-Components
Components: Blink>JavaScript>Runtime

Automatically applying components based on crash stacktrace and information from OWNERS files.

If this is incorrect, please apply the Test-Predator-Wrong-Components label.

Comment 10 by jgruber@chromium.org on Wed, Jan 13, 2021, 8:45 AM EST Project Member

Cc: leszeks@chromium.org

Comment 11 by jgruber@chromium.org on Wed, Jan 13, 2021, 8:46 AM EST Project Member

NextAction: 2021-01-20

Comment 12 by bugdroid on Wed, Jan 13, 2021, 9:16 AM EST Project Member

The following revision refers to this bug:
  https://chromium.googlesource.com/v8/v8/+/164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49

commit 164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49
Author: Jakob Gruber <jgruber@chromium.org>
Date: Wed Jan 13 14:16:06 2021

[regexp] Hard-crash on invalid offsets in AdvanceCurrentPosition

Drive-by: Range checks in `Emit(byte, twenty_four_bits)` to ensure the
given packed bits actually fit into 24 bits.

~~Bug: chromium:1166138~~
Change-Id: I2e711e6466bb48d7b9897f68dfe621d12bd92508
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2625877
Commit-Queue: Jakob Gruber <jgruber@chromium.org>
Commit-Queue: Leszek Swirski <leszeks@chromium.org>
Auto-Submit: Jakob Gruber <jgruber@chromium.org>
Reviewed-by: Leszek Swirski <leszeks@chromium.org>
Cr-Commit-Position: refs/heads/master@{#72064}

[modify] https://crrev.com/164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49/src/regexp/regexp-bytecode-generator.cc
[modify] https://crrev.com/164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49/src/regexp/regexp-bytecode-generator-inl.h
[modify] https://crrev.com/164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49/test/mjsunit/mjsunit.status
[modify] https://crrev.com/164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49/src/regexp/regexp-bytecode-generator.h
[add] https://crrev.com/164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49/test/mjsunit/regress/regress-1166138.js

Comment 13 by bugdroid on Wed, Jan 13, 2021, 10:20 AM EST Project Member

The following revision refers to this bug:
  https://chromium.googlesource.com/v8/v8/+/458f7ad06f244d76f26e460f90fdb1119a372547

commit 458f7ad06f244d76f26e460f90fdb1119a372547
Author: Nico Hartmann <nicohartmann@chromium.org>
Date: Wed Jan 13 15:19:29 2021

Revert "[regexp] Hard-crash on invalid offsets in AdvanceCurrentPosition"

This reverts commit 164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49.

Reason for revert: https://ci.chromium.org/ui/p/v8/builders/ci/V8%20Linux64%20UBSan/14532/overview

Original change's description:
> [regexp] Hard-crash on invalid offsets in AdvanceCurrentPosition
>
> Drive-by: Range checks in `Emit(byte, twenty_four_bits)` to ensure the
> given packed bits actually fit into 24 bits.
>
> ~~Bug: chromium:1166138~~
> Change-Id: I2e711e6466bb48d7b9897f68dfe621d12bd92508
> Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2625877
> Commit-Queue: Jakob Gruber <jgruber@chromium.org>
> Commit-Queue: Leszek Swirski <leszeks@chromium.org>
> Auto-Submit: Jakob Gruber <jgruber@chromium.org>
> Reviewed-by: Leszek Swirski <leszeks@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#72064}

TBR=jgruber@chromium.org,leszeks@chromium.org,pthier@chromium.org

Change-Id: Ibe72ecda03518e444442a0440ecdae7669bfc4c1
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
~~Bug: chromium:1166138~~
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2625883
Reviewed-by: Nico Hartmann <nicohartmann@chromium.org>
Commit-Queue: Nico Hartmann <nicohartmann@chromium.org>
Cr-Commit-Position: refs/heads/master@{#72065}

[modify] https://crrev.com/458f7ad06f244d76f26e460f90fdb1119a372547/src/regexp/regexp-bytecode-generator.cc
[modify] https://crrev.com/458f7ad06f244d76f26e460f90fdb1119a372547/src/regexp/regexp-bytecode-generator-inl.h
[modify] https://crrev.com/458f7ad06f244d76f26e460f90fdb1119a372547/test/mjsunit/mjsunit.status
[modify] https://crrev.com/458f7ad06f244d76f26e460f90fdb1119a372547/src/regexp/regexp-bytecode-generator.h
[delete] https://crrev.com/164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49/test/mjsunit/regress/regress-1166138.js

Comment 14 by jgruber@chromium.org on Thu, Jan 14, 2021, 1:57 AM EST Project Member

Reland in flight here https://chromium-review.googlesource.com/c/v8/v8/+/2626663/

Comment 15 by bugdroid on Thu, Jan 14, 2021, 2:38 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/ff8d0f92d423774cf773b5b4fb48b6744971e27a

commit ff8d0f92d423774cf773b5b4fb48b6744971e27a
Author: Jakob Gruber <jgruber@chromium.org>
Date: Thu Jan 14 07:37:27 2021

Reland "[regexp] Hard-crash on invalid offsets in AdvanceCurrentPosition"

This is a reland of 164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49

The reland fixes UB (left-shift of negative integer type) with a
static_cast<uint32_t>.

Original change's description:
> [regexp] Hard-crash on invalid offsets in AdvanceCurrentPosition
>
> Drive-by: Range checks in `Emit(byte, twenty_four_bits)` to ensure the
> given packed bits actually fit into 24 bits.
>
> ~~Bug: chromium:1166138~~
> Change-Id: I2e711e6466bb48d7b9897f68dfe621d12bd92508
> Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2625877
> Commit-Queue: Jakob Gruber <jgruber@chromium.org>
> Commit-Queue: Leszek Swirski <leszeks@chromium.org>
> Auto-Submit: Jakob Gruber <jgruber@chromium.org>
> Reviewed-by: Leszek Swirski <leszeks@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#72064}

Tbr: leszeks@chromium.org
~~Bug: chromium:1166138~~
Change-Id: I514495e14bb99dfc9588fdb4a9f35d67d8d64acb
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2626663
Reviewed-by: Jakob Gruber <jgruber@chromium.org>
Commit-Queue: Jakob Gruber <jgruber@chromium.org>
Cr-Commit-Position: refs/heads/master@{#72088}

[modify] https://crrev.com/ff8d0f92d423774cf773b5b4fb48b6744971e27a/src/regexp/regexp-bytecode-generator.cc
[modify] https://crrev.com/ff8d0f92d423774cf773b5b4fb48b6744971e27a/src/regexp/regexp-bytecode-generator-inl.h
[modify] https://crrev.com/ff8d0f92d423774cf773b5b4fb48b6744971e27a/test/mjsunit/mjsunit.status
[modify] https://crrev.com/ff8d0f92d423774cf773b5b4fb48b6744971e27a/src/regexp/regexp-bytecode-generator.h
[add] https://crrev.com/ff8d0f92d423774cf773b5b4fb48b6744971e27a/test/mjsunit/regress/regress-1166138.js

Comment 16 by bugdroid on Thu, Jan 14, 2021, 9:59 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/3466daa7e44c247855c10b884223321336328159

commit 3466daa7e44c247855c10b884223321336328159
Author: Patrick Thier <pthier@chromium.org>
Date: Thu Jan 14 14:58:04 2021

[regexp] Throw when length of text nodes in alternatives is too large.

Offsets in regular expressions are limited to 16 bits.
It was possible to exceed this limit when emitting greedy loops where
the length of text nodes exceeded 16 bits, resulting in overflowing
offsets.
With this CL we throw a SyntaxError "Regular expression too large" to
prevent this overflow.

~~Bug: chromium:1166138~~

Change-Id: Ica624a243bf9827083ff883d9a976f13c8da02e5
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2629286
Commit-Queue: Patrick Thier <pthier@chromium.org>
Commit-Queue: Jakob Gruber <jgruber@chromium.org>
Reviewed-by: Jakob Gruber <jgruber@chromium.org>
Cr-Commit-Position: refs/heads/master@{#72095}

[modify] https://crrev.com/3466daa7e44c247855c10b884223321336328159/test/mjsunit/mjsunit.status
[modify] https://crrev.com/3466daa7e44c247855c10b884223321336328159/src/regexp/regexp-compiler.cc
[modify] https://crrev.com/3466daa7e44c247855c10b884223321336328159/test/mjsunit/regress/regress-1166138.js

Comment 17 by jgruber@chromium.org on Thu, Jan 14, 2021, 10:18 AM EST Project Member

Status: Fixed (was: Assigned)
Owner: pthier@chromium.org

Comment 18 by ClusterFuzz on Thu, Jan 14, 2021, 12:07 PM EST Project Member

Status: Verified (was: Fixed)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5752813136445440 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_d8_dbg&range=72094:72095

If this is incorrect, please add the ClusterFuzz-Wrong label and re-open the issue.

Comment 19 by sheriffbot on Thu, Jan 14, 2021, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 20 by sheriffbot on Thu, Jan 14, 2021, 1:57 PM EST Project Member

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 21 by sheriffbot on Thu, Jan 14, 2021, 4:22 PM EST Project Member

Labels: external_security_report

Comment 22 by p4nda...@gmail.com on Mon, Jan 18, 2021, 5:38 AM EST

Hi, how about this report? Will this issue have a Security_Severity label?

Comment 23 by pthier@chromium.org on Mon, Jan 18, 2021, 10:34 AM EST Project Member

Labels: Security_Severity-Medium

This bug allows attackers to arbitrarily set the current position in the subject string (including OOB) in the regular expression interpreter. This could, potentially, lead to a memory leak.

Comment 24 by sheriffbot on Mon, Jan 18, 2021, 1:02 PM EST Project Member

Labels: Target-88 M-88

Setting milestone and target because of Security_Impact=Stable and medium severity.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 25 by sheriffbot on Mon, Jan 18, 2021, 2:22 PM EST Project Member

Labels: Merge-Request-88

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M88. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 26 by sheriffbot on Mon, Jan 18, 2021, 2:23 PM EST Project Member

Labels: -Merge-Request-88 Merge-Review-88 Hotlist-Merge-Review

This bug requires manual review: We are only 0 days from stable.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: govind@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), srinivassista @(Desktop)

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 27 by p4nda...@gmail.com on Mon, Jan 18, 2021, 10:17 PM EST

Thanks for fixing it!
And the credit info is "Bohan Liu (@P4nda20371774) and Moon Liang of Tencent Security Xuanwu Lab", if assigning a CVE number to this report.

Comment 28 by pthier@chromium.org on Wed, Jan 20, 2021, 3:59 AM EST Project Member

Labels: -Target-88 -M-88 -Merge-Review-88 Target-89 M-89

Comment 29 by pthier@chromium.org on Wed, Jan 20, 2021, 3:59 AM EST Project Member

Labels: -Hotlist-Merge-Review

Comment 30 by pthier@chromium.org on Wed, Jan 20, 2021, 4:05 AM EST Project Member

Labels: Merge-Request-89

1. Does your merge fit within the Merge Decision Guidelines?
Yes
2. Links to the CLs you are requesting to merge.
https://chromium.googlesource.com/v8/v8/+/3466daa7e44c247855c10b884223321336328159
3. Has the change landed and been verified on ToT?

Yes
4. Does this change need to be merged into other active release branches (M-1, M+1)?
No
5. Why are these changes required in this milestone after branch?
Security Bug fix
6. Is this a new feature?
No
7. If it is a new feature, is it behind a flag using finch?
No

Comment 31 by sheriffbot on Wed, Jan 20, 2021, 4:06 AM EST Project Member

Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: Reverts referenced in bugdroid comments after merge request.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 32 by adetaylor@google.com on Wed, Jan 20, 2021, 12:28 PM EST Project Member

Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89.

Comment 33 by pbommana@google.com on Wed, Jan 20, 2021, 1:10 PM EST Project Member

pthier@ change has been approved, Please go ahead and merge the CL to branch 4389 (refs/branch-heads/4389) manually asap.

Comment 34 by adetaylor@google.com on Wed, Jan 20, 2021, 7:01 PM EST Project Member

Labels: -reward-potential

Comment 35 by bugdroid on Thu, Jan 21, 2021, 6:24 AM EST Project Member

Labels: merge-merged-8.9

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/c9b71fac463dacde93fcc5ad77f56ba6ad7eeae6

commit c9b71fac463dacde93fcc5ad77f56ba6ad7eeae6
Author: Patrick Thier <pthier@chromium.org>
Date: Thu Jan 21 11:24:20 2021

[regexp] Throw when length of text nodes in alternatives is too large.

Offsets in regular expressions are limited to 16 bits.
It was possible to exceed this limit when emitting greedy loops where
the length of text nodes exceeded 16 bits, resulting in overflowing
offsets.
With this CL we throw a SyntaxError "Regular expression too large" to
prevent this overflow.

Merge of CL reviewed at https://crrev.com/c/2629286

~~Bug: chromium:1166138~~
Change-Id: Ica624a243bf9827083ff883d9a976f13c8da02e5
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2642244
Reviewed-by: Jakob Gruber <jgruber@chromium.org>
Commit-Queue: Patrick Thier <pthier@chromium.org>
Cr-Commit-Position: refs/branch-heads/8.9@{#16}
Cr-Branched-From: 16b9bbbd581c25391981aa03180b76aa60463a3e-refs/heads/8.9.255@{#1}
Cr-Branched-From: d16a2a688498bd1c3e6a49edb25d8c4ca56232dc-refs/heads/master@{#72039}

[modify] https://crrev.com/c9b71fac463dacde93fcc5ad77f56ba6ad7eeae6/src/regexp/regexp-compiler.cc
[add] https://crrev.com/c9b71fac463dacde93fcc5ad77f56ba6ad7eeae6/test/mjsunit/regress/regress-1166138.js

Comment 36 by pthier@chromium.org on Thu, Jan 21, 2021, 7:46 AM EST Project Member

Labels: -Merge-Approved-89

Comment 37 by adetaylor@google.com on Tue, Jan 26, 2021, 7:46 PM EST Project Member

Cc: anapesko@google.com

~~Issue 1166740~~ has been merged into this issue.

Comment 38 by adetaylor@google.com on Tue, Jan 26, 2021, 7:47 PM EST Project Member

VRP: this was discovered by ClusterFuzz within < 24 hours of this report.

Comment 39 by clemensb@chromium.org on Wed, Jan 27, 2021, 3:46 AM EST Project Member

I am not sure if ClusterFuzz would have found this without this report.
Note #3, where I uploaded the reproducer to CF at Jan 13, 2021, 1:35 PM GMT+1.
The mbarbella_js_mutation fuzzer then found https://clusterfuzz.com/testcase-detail/5358835920601088, but that was later.

Also, the test cases look very similar. This is the reproducer reported here:

```
let badregexp =  "(?:" +  " ".repeat(32768*2)+  ")*";
reg = RegExp(badregexp);
reg.test()
```

This is the reproducer found by mbarbella fuzzer:

```
__v_0 =  "(?:" +  " ".repeat(32768*2)+  ")*";
```

```
reg = RegExp(__v_0);
reg.test()
```

So I would say that this report should still be considered for a reward.

Comment 40 by amyressler@google.com on Wed, Feb 24, 2021, 6:40 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 41 by amyressler@google.com on Wed, Feb 24, 2021, 7:29 PM EST Project Member

Congratulations, p4nda@! The VRP Panel has decided to award you $5,000 for this report. Thank you and nice work!

Comment 42 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST Project Member

Labels: Release-0-M89

Comment 43 by amyressler@google.com on Fri, Feb 26, 2021, 3:25 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 44 by adetaylor@google.com on Mon, Mar 1, 2021, 7:27 PM EST Project Member

Labels: CVE-2021-21169 CVE_description-missing

Comment 45 by p4nda...@gmail.com on Tue, Mar 2, 2021, 9:01 PM EST

Hi, could u please modify the cred info of this report as "Bohan Liu (@P4nda20371774) and Moon Liang of Tencent Security Xuanwu Lab".

I mentioned that at previous (https://bugs.chromium.org/p/chromium/issues/detail?id=1166138#c27), It seems that too many messages have caused it to be ignored.

Comment 46 by vsavu@google.com on Wed, Mar 3, 2021, 5:32 AM EST Project Member

Labels: LTS-Merge-Request-86

Comment 47 by vsavu@google.com on Wed, Mar 3, 2021, 6:00 AM EST Project Member

Labels: LTS-Security-86

Comment 48 by gianluca@google.com on Wed, Mar 3, 2021, 10:35 AM EST Project Member

Labels: LTS-Merge-Approved-86

Comment 49 by amyressler@google.com on Wed, Mar 3, 2021, 10:54 AM EST Project Member

p4nda@ sure thing! Apologies we didn't catch that earlier. It will be updated on the release notes blog site later today.

Comment 50 by p4nda...@gmail.com on Wed, Mar 3, 2021, 9:57 PM EST

Thanks!

Comment 51 by amyressler@google.com on Tue, Mar 9, 2021, 12:58 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 52 by Git Watcher on Wed, Mar 17, 2021, 4:09 AM EDT Project Member

Labels: merge-merged-8.6

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/53c4d057974af3fde91fd960a9794533dda8204b

commit 53c4d057974af3fde91fd960a9794533dda8204b
Author: Jakob Gruber <jgruber@chromium.org>
Date: Thu Jan 14 06:55:05 2021

Reland "[regexp] Hard-crash on invalid offsets in AdvanceCurrentPosition"

This is a reland of 164cf80bbb0a6e091300bfc4cbbe70a6e6bd3e49

The reland fixes UB (left-shift of negative integer type) with a
static_cast<uint32_t>.

Original change's description:
> [regexp] Hard-crash on invalid offsets in AdvanceCurrentPosition
>
> Drive-by: Range checks in `Emit(byte, twenty_four_bits)` to ensure the
> given packed bits actually fit into 24 bits.
>
> ~~Bug: chromium:1166138~~
> Change-Id: I2e711e6466bb48d7b9897f68dfe621d12bd92508
> Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2625877
> Commit-Queue: Jakob Gruber <jgruber@chromium.org>
> Commit-Queue: Leszek Swirski <leszeks@chromium.org>
> Auto-Submit: Jakob Gruber <jgruber@chromium.org>
> Reviewed-by: Leszek Swirski <leszeks@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#72064}

(cherry picked from commit ff8d0f92d423774cf773b5b4fb48b6744971e27a)

No-Try: true
No-Presubmit: true
No-Tree-Checks: true
Tbr: leszeks@chromium.org
~~Bug: chromium:1166138~~
Change-Id: I514495e14bb99dfc9588fdb4a9f35d67d8d64acb
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2626663
Reviewed-by: Jakob Gruber <jgruber@chromium.org>
Commit-Queue: Jakob Gruber <jgruber@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#72088}

Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2742954
Reviewed-by: Jana Grill <janagrill@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/8.6@{#64}
Cr-Branched-From: a64aed2333abf49e494d2a5ce24bbd14fff19f60-refs/heads/8.6.395@{#1}
Cr-Branched-From: a626bc036236c9bf92ac7b87dc40c9e538b087e3-refs/heads/master@{#69472}

[modify] https://crrev.com/53c4d057974af3fde91fd960a9794533dda8204b/src/regexp/regexp-bytecode-generator-inl.h
[modify] https://crrev.com/53c4d057974af3fde91fd960a9794533dda8204b/src/regexp/regexp-bytecode-generator.cc
[modify] https://crrev.com/53c4d057974af3fde91fd960a9794533dda8204b/src/regexp/regexp-bytecode-generator.h
[modify] https://crrev.com/53c4d057974af3fde91fd960a9794533dda8204b/test/mjsunit/mjsunit.status
[add] https://crrev.com/53c4d057974af3fde91fd960a9794533dda8204b/test/mjsunit/regress/regress-1166138.js

Comment 53 by Git Watcher on Wed, Mar 17, 2021, 4:50 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/6e8f04c980ad9b0d91f59221107ad55e2f3b17a1

commit 6e8f04c980ad9b0d91f59221107ad55e2f3b17a1
Author: Patrick Thier <pthier@chromium.org>
Date: Thu Jan 21 10:37:10 2021

[regexp] Throw when length of text nodes in alternatives is too large.

Offsets in regular expressions are limited to 16 bits.
It was possible to exceed this limit when emitting greedy loops where
the length of text nodes exceeded 16 bits, resulting in overflowing
offsets.
With this CL we throw a SyntaxError "Regular expression too large" to
prevent this overflow.

Merge of CL reviewed at https://crrev.com/c/2629286

(cherry picked from commit c9b71fac463dacde93fcc5ad77f56ba6ad7eeae6)

No-Try: true
No-Presubmit: true
No-Tree-Checks: true
~~Bug: chromium:1166138~~
Change-Id: Ica624a243bf9827083ff883d9a976f13c8da02e5
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2642244
Reviewed-by: Jakob Gruber <jgruber@chromium.org>
Commit-Queue: Patrick Thier <pthier@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/8.9@{#16}
Cr-Original-Branched-From: 16b9bbbd581c25391981aa03180b76aa60463a3e-refs/heads/8.9.255@{#1}
Cr-Original-Branched-From: d16a2a688498bd1c3e6a49edb25d8c4ca56232dc-refs/heads/master@{#72039}
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2731531
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Jana Grill <janagrill@chromium.org>
Cr-Commit-Position: refs/branch-heads/8.6@{#68}
Cr-Branched-From: a64aed2333abf49e494d2a5ce24bbd14fff19f60-refs/heads/8.6.395@{#1}
Cr-Branched-From: a626bc036236c9bf92ac7b87dc40c9e538b087e3-refs/heads/master@{#69472}

[modify] https://crrev.com/6e8f04c980ad9b0d91f59221107ad55e2f3b17a1/src/regexp/regexp-compiler.cc
[modify] https://crrev.com/6e8f04c980ad9b0d91f59221107ad55e2f3b17a1/test/mjsunit/regress/regress-1166138.js

Comment 54 by vsavu@google.com on Thu, Mar 25, 2021, 11:53 AM EDT Project Member

Labels: -LTS-Merge-Approved-86 -LTS-Merge-Request-86 LTR-Merged-86

Comment 55 by sheriffbot on Wed, Jun 23, 2021, 1:50 PM EDT Project Member

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot