☆ Starred by 5 users

Owner:	nicohartmann@chromium.org
CC:	rzanoni@google.com tebbi@chromium.org adamk@chromium.org ishell@chromium.org gdeepti@chromium.org amyressler@chromium.org clemensb@chromium.org vahl@chromium.org ecmziegler@chromium.org ecmziegler@google.com
Status:	Verified *(Closed)*
Components:	Blink>JavaScript>Compiler>Turbofan
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
M-100
Security_Severity-Medium
Hotlist-Merge-Approved
allpublic
reward-inprocess
ClusterFuzz-Verified
CVE_description-submitted
reward-8500
external_security_report
Target-100
FoundIn-98
FoundIn-99
FoundIn-100
FoundIn-101
Security_Impact-Extended
merge-merged-9.6

LTS-Merge-Merged-96
merge-merged-10.0
Release-2-M100

Issue 1304658: Security: Debug check failed: type.representation() == MachineRepresentation::kFloat64 || type.representation() == MachineRepresentation::kTagged.

Reported by p4nda...@gmail.com on Wed, Mar 9, 2022, 6:59 AM EST

Code

This template is ONLY for reporting security bugs. If you are reporting a Download Protection Bypass bug, please use the "Security - Download Protection" template. For all other reports, please use a different template.

Please READ THIS FAQ before filing a bug: https://chromium.googlesource.com/chromium/src/+/HEAD/docs/security/faq.md

Please see the following link for instructions on filing security bugs: https://www.chromium.org/Home/chromium-security/reporting-security-bugs

Reports may be eligible for reward payments under the Chrome VRP: http://g.co/ChromeBugRewards

NOTE: Security bugs are normally made public once a fix has been widely deployed.

VULNERABILITY DETAILS
Please provide a brief explanation of the security issue.

When generating InstructionOperand at OperandForDeopt [1], if the input is NumberConstant , it will call UseImmediate.

~~~
```c++
InstructionOperand OperandForDeopt(Isolate* isolate, OperandGenerator* g,
                                   Node* input, FrameStateInputKind kind,
                                   MachineRepresentation rep) {
  if (rep == MachineRepresentation::kNone) {
    return g->TempImmediate(FrameStateDescriptor::kImpossibleValue);
  }

  switch (input->opcode()) {
    case IrOpcode::kInt32Constant:
    case IrOpcode::kInt64Constant:
    case IrOpcode::kNumberConstant:
    case IrOpcode::kFloat32Constant:
    case IrOpcode::kFloat64Constant:
    case IrOpcode::kDelayedStringConstant:
  [1]    return g->UseImmediate(input);
    case IrOpcode::kCompressedHeapConstant:
    case IrOpcode::kHeapConstant: {
      if (!CanBeTaggedOrCompressedPointer(rep)) {
        // If we have inconsistent static and dynamic types, e.g. if we
        // smi-check a string, we can get here with a heap object that
        // says it is a smi. In that case, we return an invalid instruction
~~~

```
    // operand, which will be interpreted as an optimized-out value.

    // TODO(jarin) Ideally, we should turn the current instruction
    // into an abort (we should never execute it).
    return InstructionOperand();
   }

   Handle<HeapObject> constant = HeapConstantOf(input->op());
   RootIndex root_index;
   if (isolate->roots_table().IsRootHandle(constant, &root_index) &&
     root_index == RootIndex::kOptimizedOut) {
    // For an optimized-out object we return an invalid instruction
    // operand, so that we take the fast path for optimized-out values.
    return InstructionOperand();
   }

   return g->UseImmediate(input);
  }
  case IrOpcode::kArgumentsElementsState:
  case IrOpcode::kArgumentsLengthState:
  case IrOpcode::kObjectState:
  case IrOpcode::kTypedObjectState:
   UNREACHABLE();
  default:
   switch (kind) {
    case FrameStateInputKind::kStackSlot:
     return g->UseUniqueSlot(input);
    case FrameStateInputKind::kAny:
     // Currently deopts "wrap" other operations, so the deopt's inputs
     // are potentially needed until the end of the deoptimising code.
     return g->UseAnyAtEnd(input);
   }
 }
 UNREACHABLE();
}

}  // namespace

```
In `ToConstant`[2], it will use the node->op() to generate a DeoptimizationLiteralKind::kNumber value. The NumberConstant store a tagged value, but the node->op() use its real value.

```c++
 static Constant ToConstant(const Node* node) {
  switch (node->opcode()) {
   case IrOpcode::kInt32Constant:
    return Constant(OpParameter<int32_t>(node->op()));
   case IrOpcode::kInt64Constant:
    return Constant(OpParameter<int64_t>(node->op()));
   case IrOpcode::kTaggedIndexConstant: {
    // Unencoded index value.
    intptr_t value =
      static_cast<intptr_t>(OpParameter<int32_t>(node->op()));
    DCHECK(TaggedIndex::IsValid(value));
```

```
          // Generate it as 32/64-bit constant in a tagged form.
          Address tagged_index = TaggedIndex::FromIntptr(value).ptr();
          if (kSystemPointerSize == kInt32Size) {
            return Constant(static_cast<int32_t>(tagged_index));
          } else {
            return Constant(static_cast<int64_t>(tagged_index));
          }
        }
        case IrOpcode::kFloat32Constant:
          return Constant(OpParameter<float>(node->op()));
        case IrOpcode::kRelocatableInt32Constant:
        case IrOpcode::kRelocatableInt64Constant:
          return Constant(OpParameter<RelocatablePtrConstantInfo>(node->op()));
        case IrOpcode::kFloat64Constant:
        case IrOpcode::kNumberConstant:
[2]         return Constant(OpParameter<double>(node->op()));
```

Finally, the DeoptimizationLiteral will be changed into a Number which stored at Literal Array.

```c++
Handle<Object> DeoptimizationLiteral::Reify(Isolate* isolate) const {
  Validate();
  switch (kind_) {
    case DeoptimizationLiteralKind::kObject: {
      return object_;
    }
    case DeoptimizationLiteralKind::kNumber: {
[3]       return isolate->factory()->NewNumber(number_);
    }
    case DeoptimizationLiteralKind::kString: {
      return string_->AllocateStringConstant(isolate);
    }
    case DeoptimizationLiteralKind::kInvalid: {
      UNREACHABLE();
    }
  }
  UNREACHABLE();
}
```

But when NumberConstant is the input of TypedStateValues, it may not be suitable for using Immediate.
At the case in POC, the '39: StateValues' was marked with a KRepWord32 input because of '32: Word32Shl' in SimplifiedLoweringPhase. And '68: ChangedTaggedSignedToInt32' was added as the input of '32: Word32Shl' .
After LateOptimizationPhase, the '32: Word32Shl' was removed because the '68: ChangedTaggedSignedToInt32' was replaced with `142: Word32SarShiftOutZeros`. Thus the input of '39: TypedStateValues' is '14: NumberConstant[1337]', But it was marked with a KRepWord32 input.

```cpp

Reduction MachineOperatorReducer::ReduceWord32Shl(Node* node) {
  DCHECK_EQ(IrOpcode::kWord32Shl, node->opcode());
  Int32BinopMatcher m(node);
  if (m.right().Is(0)) return Replace(m.left().node());  // x << 0 => x
  if (m.IsFoldable()) {  // K << K => K  (K stands for arbitrary constants)
    return ReplaceInt32(base::ShlWithWraparound(m.left().ResolvedValue(),
                                                m.right().ResolvedValue()));
  }
  if (m.right().IsInRange(1, 31)) {
    if (m.left().IsWord32Sar() || m.left().IsWord32Shr()) {
      Int32BinopMatcher mleft(m.left().node());

      // If x >> K only shifted out zeros:
      // (x >> K) << L => x           if K == L
      // (x >> K) << L => x >> (K-L) if K > L
      // (x >> K) << L => x << (L-K)  if K < L
      // Since this is used for Smi untagging, we currently only need it for
      // signed shifts.
      if (mleft.op() == machine()->Word32SarShiftOutZeros() &&
          mleft.right().IsInRange(1, 31)) {
        Node* x = mleft.left().node();
        int k = mleft.right().ResolvedValue();
        int l = m.right().ResolvedValue();
        if (k == l) {
          return Replace(x);
        } else if (k > l) {
          node->ReplaceInput(0, x);
          node->ReplaceInput(1, Uint32Constant(k - l));
          NodeProperties::ChangeOp(node, machine()->Word32Sar());
          return Changed(node).FollowedBy(ReduceWord32Sar(node));
        } else {
          DCHECK(k < l);
          node->ReplaceInput(0, x);
          node->ReplaceInput(1, Uint32Constant(l - k));
          return Changed(node);
        }
      }

      // (x >>> K) << K => x & ~(2^K - 1)
      // (x >> K) << K => x & ~(2^K - 1)
      if (mleft.right().Is(m.right().ResolvedValue())) {
        node->ReplaceInput(0, mleft.left().node());
        node->ReplaceInput(1,
                           Uint32Constant(std::numeric_limits<uint32_t>::max()
                                          << m.right().ResolvedValue()));
        NodeProperties::ChangeOp(node, machine()->Word32And());
        return Changed(node).FollowedBy(ReduceWord32And(node));
      }
    }
  }
  return ReduceWord32Shifts(node);
}
```

As such, it will crash at a DCHECK[3] because the type.representation() is Word32 which came from '39: TypedStateValues'
.

```c++
```

```
void CodeGenerator::AddTranslationForOperand(Instruction* instr,
                                             InstructionOperand* op,
                                             MachineType type) {
//...
  } else {
    CHECK(op->IsImmediate());
    InstructionOperandConverter converter(this, instr);
    Constant constant = converter.ToConstant(op);
    DeoptimizationLiteral literal;
    switch (constant.type()) {
// ...
  [3]    case Constant::kFloat64:
        DCHECK(type.representation() == MachineRepresentation::kFloat64 ||
               type.representation() == MachineRepresentation::kTagged);
        literal = DeoptimizationLiteral(constant.ToFloat64().value());
        break;
```

And also, it may lead to type confusion in deoptimize.

VERSION
d8 version: commit 4e9ab3a0f5387495781bf7e873586ce88441c274 ia32
Operating System: ubuntu

REPRODUCTION CASE
1. execute the attach file in d8 version.
in ia32 Debug version, it will crash with detail below:

```
#
# Fatal error in ../../src/compiler/backend/code-generator.cc, line 1351
# Debug check failed: type.representation() == MachineRepresentation::kFloat64 || type.representation() ==
MachineRepresentation::kTagged.
#
#
#
#FailureMessage Object: 0xffcd48e8
==== C stack trace ===============================
```

in release version, it will get a wrong value after deoptimize.

```
$ ./out/ia32.release/d8 --allow-natives-syntax test.js
2674
2674
1337
```

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: [tab]

I wrote a patch based on my understanding of the bug, see patch.diff .

test.js
330 bytes View Download

patch.diff
1020 bytes View Download

Comment 1 by sheriffbot on Wed, Mar 9, 2022, 7:01 AM EST

Labels: external_security_report

Comment 2 by ClusterFuzz on Wed, Mar 9, 2022, 7:59 AM EST

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5722427753299968.

Comment 3 by ClusterFuzz on Wed, Mar 9, 2022, 8:06 AM EST

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5619746762194944.

Comment 4 by ClusterFuzz on Wed, Mar 9, 2022, 8:38 AM EST

Labels: Security_Impact-Extended FoundIn-99 FoundIn-101 FoundIn-98 FoundIn-100

Detailed Report: https://clusterfuzz.com/testcase?key=5619746762194944

Fuzzer: None
Job Type: linux32_d8_dbg
Platform Id: linux

Crash Type: DCHECK failure
Crash Address:
Crash State:
  type.representation() == MachineRepresentation::kFloat64 || type.representation(

Sanitizer: address (ASAN)

Crash Revision: https://clusterfuzz.com/revisions?job=linux32_d8_dbg&revision=79142

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5619746762194944

To reproduce this, please build the target in this report and run it against the reproducer testcase. Please use the GN arguments provided at bottom of this report when building the binary.

If you have trouble reproducing, please also export the environment variables listed under "[Environment]" in the crash stacktrace.

If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 5 by bookholt@chromium.org on Wed, Mar 9, 2022, 7:25 PM EST

Owner: ishell@chromium.org
Labels: Security_Severity-Medium Pri-2

Assigning owner in addition to CCs from ClusterFuzz since @ishell has been so helpful recently. :)

Treating as Severity Medium without attempting to repo local since ClusterFuzz agrees.

Comment 6 by bookholt@chromium.org on Wed, Mar 9, 2022, 7:27 PM EST

Cc: clemensb@chromium.org

+clemensb as uploader of CF test case

Comment 7 by ishell@chromium.org on Thu, Mar 10, 2022, 5:11 AM EST

Owner: ecmziegler@chromium.org
Cc: ishell@chromium.org nicohartmann@chromium.org

Assigning to ecmziegler@ to find the right owner from the compiler team.

Comment 8 by ecmziegler@chromium.org on Thu, Mar 10, 2022, 5:47 AM EST

Owner: nicohartmann@chromium.org
Cc: -nicohartmann@chromium.org

@nicohartmann: PTAL, thank you!

Comment 9 by sheriffbot on Thu, Mar 10, 2022, 12:52 PM EST

Labels: M-100 Target-100

Setting milestone and target because of medium severity.

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

Comment 10 by sheriffbot on Thu, Mar 10, 2022, 1:18 PM EST

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 11 by sheriffbot on Thu, Mar 10, 2022, 2:22 PM EST

Status: Assigned (was: Unconfirmed)

Comment 12 by tebbi@chromium.org on Wed, Mar 16, 2022, 5:31 AM EDT

Cc: adamk@chromium.org tebbi@chromium.org gdeepti@chromium.org

~~Issue 1305573~~ has been merged into this issue.

Comment 13 by nicohartmann@chromium.org on Thu, Mar 17, 2022, 9:12 AM EDT

Status: Started (was: Assigned)

Comment 14 by nicohartmann@chromium.org on Thu, Mar 17, 2022, 11:54 AM EDT

This is pretty much the same issue as this one: https://bugs.chromium.org/p/chromium/issues/detail?id=1254189

Comment 15 by Git Watcher on Fri, Mar 18, 2022, 4:31 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/bbea5909c797dec7c620b9fee43d80a1420c2e08

commit bbea5909c797dec7c620b9fee43d80a1420c2e08
Author: Nico Hartmann <nicohartmann@chromium.org>
Date: Thu Mar 17 16:03:12 2022

[turbofan] Fix NumberConstant used with Word32 rep in ISel

~~Bug: chromium:1304658~~

Change-Id: I6a82603a7c5de5ae8f5a895990c1a904bbdd39b2
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3532263
Auto-Submit: Nico Hartmann <nicohartmann@chromium.org>
Reviewed-by: Tobias Tebbi <tebbi@chromium.org>
Commit-Queue: Tobias Tebbi <tebbi@chromium.org>
Cr-Commit-Position: refs/heads/main@{#79526}

[modify] https://crrev.com/bbea5909c797dec7c620b9fee43d80a1420c2e08/src/compiler/backend/instruction-selector.cc

Comment 16 by ClusterFuzz on Fri, Mar 18, 2022, 7:54 AM EDT

Detailed Report: https://clusterfuzz.com/testcase?key=5619746762194944

Fuzzer: None
Job Type: linux32_d8_dbg
Platform Id: linux

Crash Type: DCHECK failure
Crash Address:
Crash State:
  type.representation() == MachineRepresentation::kFloat64 || type.representation(

Sanitizer: address (ASAN)

Crash Revision: https://clusterfuzz.com/revisions?job=linux32_d8_dbg&revision=79142

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5619746762194944

To reproduce this, please build the target in this report and run it against the reproducer testcase. Please use the GN arguments provided at bottom of this report when building the binary.

If you have trouble reproducing, please also export the environment variables listed under "[Environment]" in the crash stacktrace.

If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 17 by ClusterFuzz on Fri, Mar 18, 2022, 7:55 AM EDT

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

ClusterFuzz testcase 5860360862892032 is verified as fixed in https://clusterfuzz.com/revisions?job=linux32_d8_dbg&range=79525:79526

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

Comment 18 by sheriffbot on Fri, Mar 18, 2022, 12:41 PM EDT

Labels: reward-topanel

Comment 19 by sheriffbot on Fri, Mar 18, 2022, 1:41 PM EDT

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

Comment 20 by sheriffbot on Sat, Mar 19, 2022, 12:41 PM EDT

Labels: reward-topanel

Comment 21 by sheriffbot on Sat, Mar 19, 2022, 2:10 PM EDT

Labels: Merge-Request-101 Merge-Request-100

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 M100. 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.

This is sufficiently serious that it should be merged to dev. I can't currently determine details for that channel, so please assess whether this is already merged.

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

Comment 22 by Git Watcher on Mon, Mar 21, 2022, 10:13 AM EDT

Labels: merge-merged-10.1

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/90c861ffe7fd4805959867975e5855a61c0bc341

commit 90c861ffe7fd4805959867975e5855a61c0bc341
Author: Nico Hartmann <nicohartmann@chromium.org>
Date: Thu Mar 17 16:03:12 2022

Merged: [turbofan] Fix NumberConstant used with Word32 rep in ISel

~~Bug: chromium:1304658~~

(cherry picked from commit bbea5909c797dec7c620b9fee43d80a1420c2e08)

Change-Id: Id3597bae9397805d8a46fe2eeb6fc4f6b7784b12
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3540140
Reviewed-by: Tobias Tebbi <tebbi@chromium.org>
Commit-Queue: Nico Hartmann <nicohartmann@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.1@{#4}
Cr-Branched-From: b003970395b7efcc309eb30b4ca06dd8385acd55-refs/heads/10.1.124@{#1}
Cr-Branched-From: e62f556862624103ea1da5b9dcef9b216832033b-refs/heads/main@{#79503}

[modify] https://crrev.com/90c861ffe7fd4805959867975e5855a61c0bc341/src/compiler/backend/instruction-selector.cc

Comment 23 by sheriffbot on Mon, Mar 21, 2022, 2:50 PM EDT

Labels: -Merge-Request-100 Hotlist-Merge-Review Merge-Review-100

Merge review required: M100 is already shipping to beta.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?

- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines

2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative? https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

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

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

Comment 24 by sheriffbot on Mon, Mar 21, 2022, 3:03 PM EDT

Labels: -Merge-Request-101 Hotlist-Merge-Approved Merge-Approved-101

Merge approved: your change passed merge requirements and is auto-approved for M101. Please go ahead and merge the CL to branch 4951 (refs/branch-heads/4951) manually. Please contact milestone owner if you have questions.
Merge instructions:
https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
Owners: None (Android), None (iOS), None (ChromeOS), None (Desktop)

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

Comment 25 by gov...@chromium.org on Mon, Mar 21, 2022, 3:28 PM EDT

Cc: amyressler@chromium.org
Labels: OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows

Applying all OSs except iOS as this is V8 change. Please adjust as needed.

Comment 26 by sheriffbot on Mon, Mar 21, 2022, 3:28 PM EDT

Labels: LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 27 by amyressler@chromium.org on Mon, Mar 21, 2022, 5:40 PM EDT

Labels: -merge-merged-10.1

already merged to applicable branch for M101

Comment 28 by rzanoni@google.com on Tue, Mar 22, 2022, 5:37 AM EDT

Cc: rzanoni@google.com
Labels: LTS-Evaluating-96

Comment 29 by rzanoni@google.com on Tue, Mar 22, 2022, 9:39 AM EDT

Labels: -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 30 by sheriffbot on Tue, Mar 22, 2022, 9:43 AM EDT

Labels: -LTS-Merge-Request-96 LTS-Merge-Review-96

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 31 by rzanoni@google.com on Tue, Mar 22, 2022, 9:49 AM EDT

1. Just https://crrev.com/c/3541919
2. Low, no conflicts
3. Merged to main on Mar 17, included in 10.2.x
4. Yes

Tests passing locally

Comment 32 by gmpritchard@google.com on Tue, Mar 22, 2022, 12:13 PM EDT

Labels: -LTS-Merge-Candidate LTS-Merge-Delayed-96

Comment 33 by pbommana@google.com on Tue, Mar 22, 2022, 1:43 PM EDT

Your change has been approved for M101 branch,please go ahead and merge the CL's to M101 branch manually asap so that they would be part of this week's first M99 Dev release.

Comment 34 by nicohartmann@chromium.org on Wed, Mar 23, 2022, 4:23 AM EDT

Labels: -Merge-Approved-101

Comment 35 Deleted

Comment 36 by amyressler@chromium.org on Mon, Apr 4, 2022, 6:06 PM EDT

Labels: -Merge-Review-100 Merge-Approved-100

M100 merge approved, please merge to branch 10.0-lkgr at your earliest convenience so this fix can be included in the next stable security refresh

Comment 37 by Git Watcher on Tue, Apr 5, 2022, 8:24 AM EDT

Labels: merge-merged-10.0

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/9a98f23bcabbf09525037b66a4e9202655197dc0

commit 9a98f23bcabbf09525037b66a4e9202655197dc0
Author: Nico Hartmann <nicohartmann@chromium.org>
Date: Thu Mar 17 16:03:12 2022

Merged: [turbofan] Fix NumberConstant used with Word32 rep in ISel

~~Bug: chromium:1304658~~
(cherry picked from commit bbea5909c797dec7c620b9fee43d80a1420c2e08)

Change-Id: I721b07f434128d9fdf9fbd05932214e0a14e56c7
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3540120
Reviewed-by: Tobias Tebbi <tebbi@chromium.org>
Commit-Queue: Nico Hartmann <nicohartmann@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.0@{#22}
Cr-Branched-From: 6ea73a738c467dc26abbbe84e27a36aac1c6e119-refs/heads/10.0.139@{#1}
Cr-Branched-From: ccc689011280419901e6ee42cae39980c0e96030-refs/heads/main@{#79131}

[modify] https://crrev.com/9a98f23bcabbf09525037b66a4e9202655197dc0/src/compiler/backend/instruction-selector.cc

Comment 38 by nicohartmann@chromium.org on Tue, Apr 5, 2022, 8:30 AM EDT

Labels: -Merge-Approved-100

Comment 39 by gmpritchard@google.com on Fri, Apr 8, 2022, 11:29 AM EDT

Labels: -LTS-Merge-Review-96 -LTS-Merge-Delayed-96 LTS-Merge-Approved-96

Comment 40 by Git Watcher on Mon, Apr 11, 2022, 8:45 AM EDT

Labels: merge-merged-9.6

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/2004594a46c8a2766de63d850d15fcf5efe82dc9

commit 2004594a46c8a2766de63d850d15fcf5efe82dc9
Author: Nico Hartmann <nicohartmann@chromium.org>
Date: Thu Mar 17 16:03:12 2022

[M96-LTS][turbofan] Fix NumberConstant used with Word32 rep in ISel

~~Bug: chromium:1304658~~

(cherry picked from commit bbea5909c797dec7c620b9fee43d80a1420c2e08)

No-Try: true
No-Presubmit: true
No-Tree-Checks: true
Change-Id: I6a82603a7c5de5ae8f5a895990c1a904bbdd39b2
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3532263

Auto-Submit: Nico Hartmann <nicohartmann@chromium.org>
Commit-Queue: Tobias Tebbi <tebbi@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#79526}
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3541919
Reviewed-by: Nico Hartmann <nicohartmann@chromium.org>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/9.6@{#58}
Cr-Branched-From: 0b7bda016178bf438f09b3c93da572ae3663a1f7-refs/heads/9.6.180@{#1}
Cr-Branched-From: 41a5a247d9430b953e38631e88d17790306f7a4c-refs/heads/main@{#77244}

[modify] https://crrev.com/2004594a46c8a2766de63d850d15fcf5efe82dc9/src/compiler/backend/instruction-selector.cc

Comment 41 by rzanoni@google.com on Mon, Apr 11, 2022, 8:48 AM EDT

Labels: -LTS-Merge-Approved-96 LTS-Merge-Merged-96

Comment 42 by adetaylor@google.com on Mon, Apr 11, 2022, 1:15 PM EDT

Labels: Release-2-M100

Comment 43 by adetaylor@google.com on Mon, Apr 11, 2022, 1:30 PM EDT

Labels: CVE-2022-1314 CVE_description-missing

Comment 44 by p4nda...@gmail.com on Mon, Apr 11, 2022, 4:19 PM EDT

Sorry, may I modify the credit info as "Bohan Liu (@P4nda20371774) and exp-sky of Tencent Security Xuanwu Lab"?

I would be very grateful if it could be modified!!

Comment 45 by amyressler@google.com on Fri, Apr 15, 2022, 1:09 PM EDT

Labels: -reward-topanel reward-unpaid reward-8500

*** 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 46 by amyressler@chromium.org on Fri, Apr 15, 2022, 1:18 PM EDT

Congratulations, Bohan Liu and exp-sky! The VRP Panel have decided to award you $7500 for this report +$1,000 patch bonus. Thank you for your efforts and reporting this issue to us!

Comment 47 by amyressler@google.com on Fri, Apr 15, 2022, 9:55 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 48 by sheriffbot on Fri, Jun 24, 2022, 1:31 PM EDT

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

Comment 49 by amyressler@google.com on Tue, Jul 26, 2022, 4:57 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 50 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy