



☆ Starred by 1 user

Owner:	 yosin@chromium.org Back on Jan 10
CC:	rakina@chromium.org xiaoc...@chromium.org janag...@google.com  yosin@chromium.org mbarb...@chromium.org mas...@chromium.org
Status:	Verified (Closed)
Components:	Blink>Editing
Modified:	Feb 9, 2021
Backlog-Rank:	---
Editors:	---
EstimatedDays:	---
NextAction:	---
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-2000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
ClusterFuzz-Verified
CVE_description-submitted
Target-88
Target-87
FoundIn-83
FoundIn-84
M-88
Merge-Rejected-87
merge-merged-4240
merge-merged-86
LTC-Merged-86
LTS-Security-86
Release-0-M88
CVE-2021-21128

Issue 1138877: Security: heap-buffer-overflow in window.find
Reported by liangdong46@gmail.com on Thu, Oct 15, 2020, 8:51 AM EDT

 Code

VULNERABILITY DETAILS

VERSION
Chrome Version: 83.0.4103.97 stable
Operating System: Linux

REPRODUCTION CASE
browse the attached file

CREDIT INFORMATION
Reporter credit: Liang Dong

```
==1==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200008d016 at pc 0x5598111fad5e bp 0x7ffe7d21b0f0 sp 0x7ffe7d21b0e8
READ of size 2 at 0x60200008d016 thread T0 (chrome)
==1==WARNING: invalid path to external symbolizer!
==1==WARNING: Failed to use and restart external symbolizer!
#0 0x5598111fad5d in blink::IsWholeWordMatch(unsigned short const*, int, blink::MatchResultICU&)
./././third_party/blink/renderer/core/editing/iterators/text_searcher_icu.cc:109:3
#1 0x5598111fad5d in blink::TextSearcherICU::ShouldSkipCurrentMatch(blink::MatchResultICU&) const
./././third_party/blink/renderer/core/editing/iterators/text_searcher_icu.cc:211:35
#2 0x5598111fa778 in blink::TextSearcherICU::NextMatchResult(blink::MatchResultICU&) ./././third_party/blink/renderer/core/editing/iterators/text_searcher_icu.cc:170:10
#3 0x5598111b74fd in blink::FindBuffer::Results::Iterator::operator++() ./././third_party/blink/renderer/core/editing/finder/find_buffer.cc:500:32
#4 0x5598111b74fd in blink::FindBuffer::Results::Iterator::Iterator(blink::FindBuffer const&, blink::TextSearcherICU*, WTF::String const&)
./././third_party/blink/renderer/core/editing/finder/find_buffer.cc:489:3
#5 0x5598111b74fd in blink::FindBuffer::Results::begin() const ./././third_party/blink/renderer/core/editing/finder/find_buffer.cc:451:10
#6 0x5598111b74fd in blink::FindBuffer::Results::IsEmpty() const ./././third_party/blink/renderer/core/editing/finder/find_buffer.cc:459:10
#7 0x5598111b74fd in blink::FindBuffer::FindMatchInRange(blink::EphemeralRangeTemplate<blink::EditingAlgorithm<blink::FlatTreeTraversal> > const&, WTF::String,
unsigned int) ./././third_party/blink/renderer/core/editing/finder/find_buffer.cc:171:24
#8 0x5598110d8c04 in blink::FindStringBetweenPositions(WTF::String const&, blink::EphemeralRangeTemplate<blink::EditingAlgorithm<blink::FlatTreeTraversal> >
const&, unsigned int) ./././third_party/blink/renderer/core/editing/editor.cc:780:9
#9 0x5598110d7fba in blink::Editor::FindRangeOfString(blink::Document&, WTF::String const&,
blink::EphemeralRangeTemplate<blink::EditingAlgorithm<blink::FlatTreeTraversal> > const&, unsigned int, bool*) ./././third_party/blink/renderer/core/editing/editor.cc:848:7
#10 0x5598110d792b in blink::Editor::FindString(blink::LocalFrame&, WTF::String const&, unsigned int) ./././third_party/blink/renderer/core/editing/editor.cc:751:31
#11 0x559816b00588 in blink::(anonymous namespace)::FindOperationCallback(v8::FunctionCallbackInfo<v8::Value> const&)
./gen/third_party/blink/renderer/bindings/modules/v8/v8_window.cc:17966:41
#12 0x5598014f9f6d in v8::internal::FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) ./././v8/src/api/api-arguments-inl.h:158:3
#13 0x55980147fa35 in v8::internal::MaybeHandle<v8::internal::Object> v8::internal::(anonymous namespace)::HandleApiCallHelper<false>(v8::internal::Isolate*,
v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::FunctionTemplateInfo>,
v8::internal::Handle<v8::internal::Object>, v8::internal::BuiltinArguments) ./././v8/src/builtins/builtins-api.cc:111:36
#14 0x5598014f559e in v8::internal::Builtin_Impl_HandleApiCall(v8::internal::BuiltinArguments, v8::internal::Isolate*) ./././v8/src/builtins/builtins-api.cc:141:5
#15 0x55980360c237 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit ??:0:0
#16 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#17 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
```

```
#18 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#19 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#20 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#21 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#22 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#23 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#24 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#25 0x55980359c35a in Builtins_JSEntryTrampoline ??:0:0
#26 0x55980359c137 in Builtins_JSEntry ??:0:0
#27 0x55980178ce60 in v8::internal:GeneratedCode<unsigned long, unsigned long, unsigned long, unsigned long, unsigned long, long, unsigned long*>::Call(unsigned
long, unsigned long, unsigned long, unsigned long, long, unsigned long**) J.J./v8/src/execution/simulator.h:142:12
#28 0x55980178ce60 in v8::internal:(anonymous namespace)::Invoke(v8::internal::Isolate*, v8::internal:(anonymous namespace)::InvokeParams const&)
J.J./v8/src/execution/execution.cc:368:33
#29 0x55980178bd00 in v8::internal:Execution::Call(v8::internal::Isolate*, v8::internal::Handle<v8::internal::Object>, v8::internal::Handle<v8::internal::Object>, int,
v8::internal::Handle<v8::internal::Object*>) J.J./v8/src/execution/execution.cc:462:10
#30 0x5598013d1b52 in v8::Function::Call(v8::Local<v8::Context>, v8::Local<v8::Value>, int, v8::Local<v8::Value*>) J.J./v8/src/api/api.cc:5007:7
#31 0x55980fe92424 in blink::V8ScriptRunner::CallFunction(v8::Local<v8::Function>, blink::ExecutionContext*, v8::Local<v8::Value>, int, v8::Local<v8::Value*>,
v8::Isolate*) J.J./third_party/blink/renderer/bindings/core/v8/v8_script_runner.cc:629:17
#32 0x5598115b0e07 in blink::V8Function::Invoke(blink::bindings::V8ValueOrScriptWrappableAdapter, blink::HeapVector<blink::ScriptValue, 0u> const&)
Jgen/third_party/blink/renderer/bindings/core/v8/v8_function.cc:107:8
#33 0x5598115b194c in blink::V8Function::InvokeAndReportException(blink::bindings::V8ValueOrScriptWrappableAdapter, blink::HeapVector<blink::ScriptValue, 0u>
const&) Jgen/third_party/blink/renderer/bindings/core/v8/v8_function.cc:251:7
#34 0x5598115af5ae in blink::ScheduledAction::Execute(blink::ExecutionContext*) J.J./third_party/blink/renderer/bindings/core/v8/scheduled_action.cc:130:16
#35 0x5598115ad783 in blink::DOMTimer::Fired() J.J./third_party/blink/renderer/core/frame/dom_timer.cc:209:11
#36 0x55980da330a in blink::TimerBase::RunInternal() J.J./third_party/blink/renderer/platform/timer.cc:152:3
#37 0x559804993cc5 in base::OnceCallback<void (*)>::Run() && J.J./base/callback.h:100:12
#38 0x559804993cc5 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) J.J./base/task/common/task_annotator.cc:163:33
#39 0x5598049cbb9f in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
J.J./base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:332:23
#40 0x5598049cb41f in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
J.J./base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:252:36
#41 0x5598048c2f6d in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) J.J./base/message_loop/message_pump_default.cc:39:55
#42 0x5598049cfd00 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
J.J./base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:446:12
#43 0x559804940c9a in base::RunLoop::Run() J.J./base/run_loop.cc:124:14
#44 0x5598175c551c in content::RendererMain(content::MainFunctionParams const&) J.J./content/renderer/renderer_main.cc:256:16
#45 0x5598046ca22e in content::RunZygote(content::ContentMainDelegate*) J.J./content/app/content_main_runner_impl.cc:485:14
#46 0x5598046cdc6d in content::ContentMainRunnerImpl::Run(bool) J.J./content/app/content_main_runner_impl.cc:860:10
#47 0x5598046c70a1 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) J.J./content/app/content_main.cc:373:36
#48 0x5598046c76cc in content::ContentMain(content::ContentMainParams const&) J.J./content/app/content_main.cc:399:10
#49 0x5597fa42d165 in ChromeMain J.J./chrome/app/chrome_main.cc:130:12
#50 0x7f3a858af0b2 in __libc_start_main /build/glibc-ZN95T4/glibc-2.31/csu/_libc-start.c:308:16

0x60200008d016 is located 0 bytes to the right of 6-byte region [0x60200008d010,0x60200008d016)
allocated by thread T0 (chrome) here:
#0 0x5597fa40101d in malloc /b/s/wir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_malloc_linux.cpp:145:3
#1 0x559809c8b9bd in base::PartitionRoot<true>::AllocFlags(int, unsigned long, char const*) J.J./base/allocator/partition_allocator/partition_alloc.h:941:48
#2 0x559809c8b9bd in base::PartitionRoot<true>::Alloc(unsigned long, char const*) J.J./base/allocator/partition_allocator/partition_alloc.h:1162:10
#3 0x559809c8b9bd in WTF::Partitions::BufferMalloc(unsigned long, char const*) J.J./third_party/blink/renderer/platform/wtf/allocator/partitions.cc:226:29
#4 0x559800dc3631 in unsigned short* WTF::PartitionAllocator::AllocateVectorBacking<unsigned short>(unsigned long)
J.J./third_party/blink/renderer/platform/wtf/allocator/partition_allocator.h:38:9
#5 0x559800dc3631 in WTF::VectorBufferBase<unsigned short, WTF::PartitionAllocator>::AllocateBufferNoBarrier(unsigned int)
J.J./third_party/blink/renderer/platform/wtf/vector.h:490:9
#6 0x559800dc3631 in WTF::VectorBufferBase<unsigned short, WTF::PartitionAllocator>::AllocateTemporaryBuffer(unsigned int)
J.J./third_party/blink/renderer/platform/wtf/vector.h:550:12
#7 0x559800dc3631 in WTF::Vector<unsigned short, 0u, WTF::PartitionAllocator>::ReallocateBuffer(unsigned int)
J.J./third_party/blink/renderer/platform/wtf/vector.h:2207:7
#8 0x559803948376 in WTF::Vector<unsigned short, 0u, WTF::PartitionAllocator>::ReserveCapacity(unsigned int)
J.J./third_party/blink/renderer/platform/wtf/vector.h:1808:3
#9 0x559803948376 in WTF::Vector<unsigned short, 0u, WTF::PartitionAllocator>::ExpandCapacity(unsigned int)
J.J./third_party/blink/renderer/platform/wtf/vector.h:1721:3
#10 0x559803948376 in WTF::Vector<unsigned short, 0u, WTF::PartitionAllocator>::ExpandCapacity(unsigned int, unsigned short*)
J.J./third_party/blink/renderer/platform/wtf/vector.h:1730:5
#11 0x559803948376 in WTF::Vector<unsigned short, 0u, WTF::PartitionAllocator>::ExpandCapacity(unsigned int, unsigned short const*)
J.J./third_party/blink/renderer/platform/wtf/vector.h:1441:12
#12 0x559803948376 in void WTF::Vector<unsigned short, 0u, WTF::PartitionAllocator>::Append<unsigned short>(unsigned short const*, unsigned int)
J.J./third_party/blink/renderer/platform/wtf/vector.h:1900:12
#13 0x5598111bb86d in blink::FindBuffer::AddTextToBuffer(blink::Text const&, blink::LayoutBlockFlow&,
blink::EphemeralRangeTemplate<blink::EditingAlgorithm<blink::FlatTreeTraversal>> > const&) J.J./third_party/blink/renderer/core/editing/finder/find_buffer.cc:422:13
#14 0x5598111b631f in blink::FindBuffer::CollectTextUntilBlockBoundary(blink::EphemeralRangeTemplate<blink::EditingAlgorithm<blink::FlatTreeTraversal> > const&)
J.J./third_party/blink/renderer/core/editing/finder/find_buffer.cc:321:7
#15 0x5598111b72c1 in blink::FindBuffer::FindBuffer(blink::EphemeralRangeTemplate<blink::EditingAlgorithm<blink::FlatTreeTraversal> > const&)
J.J./third_party/blink/renderer/core/editing/finder/find_buffer.cc:117:3
#16 0x5598111b72c1 in blink::FindBuffer::FindMatchInRange(blink::EphemeralRangeTemplate<blink::EditingAlgorithm<blink::FlatTreeTraversal> > const&, WTF::String,
unsigned int) J.J./third_party/blink/renderer/core/editing/finder/find_buffer.cc:168:16
#17 0x5598110d8c04 in blink::FindStringBetweenPositions(WTF::String const&, blink::EphemeralRangeTemplate<blink::EditingAlgorithm<blink::FlatTreeTraversal> >
const&, unsigned int) J.J./third_party/blink/renderer/core/editing/editor.cc:780:9
#18 0x5598110d7fba in blink::Editor::FindRangeOfString(blink::Document&, WTF::String const&,
blink::EphemeralRangeTemplate<blink::EditingAlgorithm<blink::FlatTreeTraversal> > const&, unsigned int, bool) J.J./third_party/blink/renderer/core/editing/editor.cc:848:7
#19 0x5598110d792b in blink::Editor::FindString(blink::LocalFrame&, WTF::String const&, unsigned int) J.J./third_party/blink/renderer/core/editing/editor.cc:751:31
#20 0x5598116b00588 in blink:(anonymous namespace)::FindOperationCallback(v8::FunctionCallbackInfo<v8::Value> const&)
Jgen/third_party/blink/renderer/bindings/modules/v8/v8_window.cc:1796:41
#21 0x5598014f96fd in v8::internal:FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) J.J./v8/src/api/api-arguments-inl.h:158:3
#22 0x55980147af35 in v8::internal:MaybeHandle<v8::internal::Object> v8::internal:(anonymous namespace)::HandleApiCallHelper<false>(v8::internal::Isolate*,
v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::FunctionTemplateInfo>,
v8::internal::Handle<v8::internal::Object>, v8::internal::BuiltinArguments) J.J./v8/src/builtins/builtins-api.cc:111:36
#23 0x5598014f559e in v8::internal:Builtin_Impl_HandleApiCal(v8::internal::BuiltinArguments, v8::internal::Isolate*) J.J./v8/src/builtins/builtins-api.cc:141:5
#24 0x55980360c237 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit ??:0:0
#25 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#26 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#27 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#28 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#29 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#30 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#31 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#32 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#33 0x55980359e837 in Builtins_InterpreterEntryTrampoline ??:0:0
#34 0x55980359c35a in Builtins_JSEntryTrampoline ??:0:0
#35 0x55980359c137 in Builtins_JSEntry ??:0:0
#36 0x55980178ce60 in v8::internal:GeneratedCode<unsigned long, unsigned long, unsigned long, unsigned long, unsigned long, long, unsigned long*>::Call(unsigned
long, unsigned long, unsigned long, unsigned long, long, unsigned long**) J.J./v8/src/execution/simulator.h:142:12
#37 0x55980178ce60 in v8::internal:(anonymous namespace)::Invoke(v8::internal::Isolate*, v8::internal:(anonymous namespace)::InvokeParams const&)
J.J./v8/src/execution/execution.cc:368:33
```

```
#38 0x55980178bde0 in v8::internal::Execution::Call(v8::internal::Isolate*, v8::internal::Handle<v8::internal::Object>, v8::internal::Handle<v8::internal::Object>, int, v8::internal::Handle<v8::internal::Object*>) J.J./v8/src/execution/execution.cc:462:10
#39 0x5598013d1b52 in v8::Function::Call(v8::Local<v8::Context>, v8::Local<v8::Value>, int, v8::Local<v8::Value>*) J.J./v8/src/api/api.cc:5007:7
#40 0x55980fe92424 in blink::V8ScriptRunner::CallFunction(v8::Local<v8::Function>, blink::ExecutionContext*, v8::Local<v8::Value>, int, v8::Local<v8::Value>*, v8::Isolate*) J.J./third_party/blink/renderer/bindings/core/v8/v8_script_runner.cc:629:17
```

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/dev/Downloads/chromium_src/src/out/asan/chrome+0x20917d5d)
Shadow bytes around the buggy address:

```
0x0c04800099b0: fa fa 05 fa fa 00 06 fa fa fd fa fa fd fa
0x0c04800099c0: fa fa fd fa fa fd fa fa fd fa fa 01 fa
0x0c04800099d0: fa fa 01 fa fa 06 fa fa 06 fa fa fd fa
0x0c04800099e0: fa fa fd fa fa fd fd fa fd fa fd fa
0x0c04800099f0: fa fa fd fa fa fd fa fa 00 00 fa fa fd fd
=>0x0c0480009a00: fa fa[06]fa fa fa fa fa fa fa fa fa fa
0x0c0480009a10: fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0480009a20: fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0480009a30: fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0480009a40: fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0480009a50: 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

heap-buffer-overflow.html
279 bytes [View](#) [Download](#)

Comment 1 by [ClusterFuzz](#) on Thu, Oct 15, 2020, 2:09 PM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5767959052353536>.

Comment 2 by [palmer@chromium.org](#) on Thu, Oct 15, 2020, 2:10 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: [rakina@chromium.org](#)
Cc: [yosin@chromium.org](#) [xiaoc...@chromium.org](#) [rakina@chromium.org](#)
Labels: Security_Impact-Stable OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows Pri-1
Components: Blink>Editing

[rakina](#), it looks like you last worked on the code at the top of the stack. Could you please take a look? Thank you!

Comment 3 by [ClusterFuzz](#) on Fri, Oct 16, 2020, 1:09 AM EDT Project Member

Labels: FoundIn-83 FoundIn-84 Security_Severity-Medium

Detailed Report: <https://clusterfuzz.com/testcase?key=5767959052353536>

Fuzzer: None
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Heap-buffer-overflow READ 2
Crash Address: 0x60900023fff4
Crash State:
blink::TextSearcher(CU::ShouldSkipCurrentMatch
blink::TextSearcher(CU::NextMatchResult
blink::FindBuffer::FindMatchInRange

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=628682:628683

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5767959052353536

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/5767959052353536> -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/Yh3qCYFvHj6E5jz5> so we can improve.

A recommended severity was added to this bug. Please change the severity if it is inaccurate.

Comment 4 by [rakina@chromium.org](#) on Fri, Oct 16, 2020, 1:29 AM EDT Project Member

Owner: [yosin@chromium.org](#)
Hmm, there might be some unicode-related subtleties here. We overflowed trying to get the text with U16_GET:
https://source.chromium.org/chromium/chromium/src/+master:third_party/blink/renderer/core/editing/iterators/text_searcher_icu.cc;l=109;drc=fd343439bf9582a4f3c21276893a9c081e29929c. I'm re-assigning to [yosin@](#) who should know more than I do on this.

Comment 5 by [yosin@chromium.org](#) on Fri, Oct 16, 2020, 3:06 AM EDT Project Member

Status: Started (was: Assigned)

In review: <http://crrev.com/c/2476878>

Comment 6 by [bugdroid](#) on Fri, Oct 16, 2020, 4:43 AM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+93a75877b2db7f00e94f9c8619a26e6777ce3f11>

commit [93a75877b2db7f00e94f9c8619a26e6777ce3f11](#)

Author: Yoshifumi Inoue <yosin@chromium.org>

Date: Fri Oct 16 08:41:24 2020

[FindInPage] Make `IsWholeWordMatch()` to use `U16_GET()` with valid parameter

This patch chagnes `|IsWholeWordMatch()|` to use `|U16_GET()|` with valid parameters to avoid reading out of bounds data.

In case of search "uDB00" (broken surrogate pair) in "u0022uDB00", we call `|U16_GET(text, start, index, length, u32)|` with `start=1, index=1, length=1`, where `text = "u0022DB800"`, then `|U16_GET()|` reads `text[2]` for surrogate tail.

After this patch, we call `|U16_GET()|` with `length=2==end of match`, to make `|U16_GET()|` not to read `text[2]`.

~~Bug: 1428872~~

Change-Id: [I3407f795ab181edc7d0f1d1f0a0d380974cd34eb](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2476878>

Auto-Submit: Yoshifumi Inoue <yosin@chromium.org>

Reviewed-by: Rakina Zata Amni <rakina@chromium.org>

Commit-Queue: Rakina Zata Amni <rakina@chromium.org>

Commit-Queue: Yoshifumi Inoue <yosin@chromium.org>

Cr-Commit-Position: refs/heads/master@{#817847}

[modify] https://crrev.com/93a75877b2db7f00e94f9c8619a26e6777ce3f11/third_party/blink/renderer/core/editing/iterators/text_searcher_icu.cc

[modify] https://crrev.com/93a75877b2db7f00e94f9c8619a26e6777ce3f11/third_party/blink/renderer/core/editing/iterators/text_searcher_icu_test.cc

Comment 7 by [sheriffbot](#) on Fri, Oct 16, 2020, 2:13 PM EDT Project Member

Labels: M-87 Target-87

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 8 by [ClusterFuzz](#) on Sun, Oct 18, 2020, 9:22 PM EDT Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5767959052353536>

Fuzzer: None

Job Type: linux_asan_chrome_mp

Platform Id: linux

Crash Type: Heap-buffer-overflow READ 2

Crash Address: 0x60900023fff4

Crash State:

blink::TextSearcherICU::ShouldSkipCurrentMatch

blink::TextSearcherICU::NextMatchResult

blink::FindBuffer::FindMatchInRange

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=628682:628683

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5767959052353536

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/5767959052353536 -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 Sun, Oct 18, 2020, 9:47 PM EDT Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5767959052353536>

Fuzzer: None

Job Type: linux_asan_chrome_mp

Platform Id: linux

Crash Type: Heap-buffer-overflow READ 2

Crash Address: 0x60900023fff4

Crash State:

blink::TextSearcherICU::ShouldSkipCurrentMatch

blink::TextSearcherICU::NextMatchResult

blink::FindBuffer::FindMatchInRange

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=628682:628683

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5767959052353536

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/5767959052353536 -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 10](#) by ClusterFuzz on Mon, Oct 19, 2020, 3:42 AM EDT Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5767959052353536>

Fuzzer: None
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Heap-buffer-overflow READ 2
Crash Address: 0x60900023fff4
Crash State:
blink::TextSearcher(CU)::ShouldSkipCurrentMatch
blink::TextSearcher(CU)::NextMatchResult
blink::FindBuffer::FindMatchInRange

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=628682:628683

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5767959052353536

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/5767959052353536 -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 11](#) by ClusterFuzz on Mon, Oct 19, 2020, 8:58 PM EDT Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5767959052353536>

Fuzzer: None
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Heap-buffer-overflow READ 2
Crash Address: 0x60900023fff4
Crash State:
blink::TextSearcher(CU)::ShouldSkipCurrentMatch
blink::TextSearcher(CU)::NextMatchResult
blink::FindBuffer::FindMatchInRange

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=628682:628683

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5767959052353536

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/5767959052353536 -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 12](#) by yosin@chromium.org on Mon, Oct 19, 2020, 9:06 PM EDT Project Member

Status: Fixed (was: Started)

[Comment 13](#) by ClusterFuzz on Mon, Oct 19, 2020, 9:08 PM EDT Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5767959052353536>

Fuzzer: None
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Heap-buffer-overflow READ 2
Crash Address: 0x60900023fff4
Crash State:
blink::TextSearcher(CU)::ShouldSkipCurrentMatch
blink::TextSearcher(CU)::NextMatchResult
blink::FindBuffer::FindMatchInRange

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=628682:628683

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5767959052353536

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/5767959052353536 -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 14](#) by [sheriffbot](#) on Tue, Oct 20, 2020, 1:55 PM EDT Project Member

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

[Comment 15](#) by [ClusterFuzz](#) on Tue, Oct 20, 2020, 10:17 PM EDT Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5767959052353536>

Fuzzer: None

Job Type: linux_asan_chrome_mp

Platform Id: linux

Crash Type: Heap-buffer-overflow READ 2

Crash Address: 0x60900023fff4

Crash State:

blink::TextSearcherICU::ShouldSkipCurrentMatch

blink::TextSearcherICU::NextMatchResult

blink::FindBuffer::FindMatchInRange

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=628682:628683

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5767959052353536

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/5767959052353536 -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 16](#) by [ClusterFuzz](#) on Wed, Oct 21, 2020, 3:47 PM EDT Project Member

Status: Verified (was: Fixed)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5767959052353536 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=817421:819253

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

[Comment 17](#) by [ClusterFuzz](#) on Wed, Oct 21, 2020, 9:06 PM EDT Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5767959052353536>

Fuzzer: None

Job Type: linux_asan_chrome_mp

Platform Id: linux

Crash Type: Heap-buffer-overflow READ 2

Crash Address: 0x60900023fff4

Crash State:

blink::TextSearcherICU::ShouldSkipCurrentMatch

blink::TextSearcherICU::NextMatchResult

blink::FindBuffer::FindMatchInRange

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=628682:628683

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5767959052353536

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/5767959052353536 -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 18](#) by [adetaylor@google.com](#) on Mon, Oct 26, 2020, 12:04 PM EDT Project Member

Labels: reward-topanel

[Comment 19](#) by [adetaylor@google.com](#) on Mon, Oct 26, 2020, 12:21 PM EDT Project Member

Cc: mbarb...@chromium.org

mbarbella@ is there any way to request a finer grained fix range after the recent ASAN outage (see the huge range in [#c16](#))? There are several bugs which are going to be time-consuming to discuss at the VRP as we don't know which CL fixed them, so I can't check for duplicates.

[Comment 20](#) by [sheriffbot](#) on Mon, Oct 26, 2020, 2:21 PM EDT Project Member

Labels: Merge-Request-87

Requesting merge to beta M87 because latest trunk commit (817847) appears to be after beta branch point (812852).

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

[Comment 21](#) by [sheriffbot](#) on Mon, Oct 26, 2020, 2:24 PM EDT Project Member

Labels: -Merge-Request-87 Merge-Review-87 Hotlist-Merge-Review

This bug requires manual review: M87's targeted beta branch promotion date has already passed, so this requires manual review
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), bindusuvama @(iOS), cindyb@(ChromeOS), lakpamathy@(Desktop)

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

Comment 22 by mbarb...@chromium.org on Mon, Oct 26, 2020, 3:51 PM EDT Project Member

Re #c19: I can't think of anything simple that would work well. On the off chance that any of the bugs can be reproduced on jobs that didn't break, re-uploading to those is the only thing I can think of that would help, but I don't expect that to be likely.

Comment 23 by adetaylor@google.com on Tue, Oct 27, 2020, 6:13 PM EDT Project Member

Labels: -Merge-Review-87 Merge-Rejected-87

Thanks mbarbella@. yosin@, can you help identify how this was fixed?

Rejecting merge to M87 because it's not clear what we should merge.

Comment 24 by adetaylor@google.com on Wed, Oct 28, 2020, 6:55 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-2000

*** 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 25 by adetaylor@google.com on Wed, Oct 28, 2020, 7:12 PM EDT Project Member

Congratulations! The VRP panel has awarded \$2000 for this bug.

Comment 26 by adetaylor@google.com on Thu, Oct 29, 2020, 10:27 AM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 27 by adetaylor@google.com on Wed, Jan 13, 2021, 5:48 PM EST Project Member

Labels: Release-0-M88

Comment 28 by amyressler@google.com on Tue, Jan 19, 2021, 1:56 PM EST Project Member

Labels: CVE-2021-21128 CVE_description-missing

Comment 29 by janag...@google.com on Wed, Jan 20, 2021, 7:31 AM EST Project Member

Cc: janag...@google.com

Labels: LTS-Security-86 Merge-Request-86-LTS

Comment 30 by gianluca@google.com on Wed, Jan 20, 2021, 12:01 PM EST Project Member

Labels: Merge-Approved-86-LTS

Comment 31 by sheriffbot on Wed, Jan 20, 2021, 12:22 PM EST Project Member

Labels: -M-87 Target-88 M-88

Comment 32 by bugdroid on Fri, Jan 22, 2021, 5:09 AM EST Project Member

Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+e75cf1792dba812a4e43a928e275f6d83df8b961>

commit [e75cf1792dba812a4e43a928e275f6d83df8b961](#)

Author: Yoshifumi Inoue <yosin@chromium.org>

Date: Fri Jan 22 10:09:22 2021

[FindInPage] Make IsWholeWordMatch() to use U16_GET() with valid parameter

This patch chagnes |IsWholeWordMatch| to use |U16_GET| with valid parameters to avoid reading out of bounds data.

In case of search "uDB00" (broken surrogate pair) in "u0022uDB00", we call |U16_GET(text, start, index, length, u32)| with start=1, index=1, length=1, where text = "u0022DB00", then |U16_GET| reads text[2] for surrogate tail.

After this patch, we call |U16_GET| with length=2==end of match, to make |U16_GET| not to read text[2].

(cherry picked from commit [93a75877b2db7f00e949c8619a26e6777ce3f11](#))

Bug: [4439877](#)

Change-Id: [I3407f795ab181edc7d0f1d1f0a0d380974cd34eb](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2476878>

Auto-Submit: Yoshifumi Inoue <yosin@chromium.org>

Reviewed-by: Rakina Zata Amni <rakina@chromium.org>

Commit-Queue: Rakina Zata Amni <rakina@chromium.org>
Commit-Queue: Yoshifumi Inoue <yosin@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#817847}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2640057>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Yoshifumi Inoue <yosin@chromium.org>
Commit-Queue: Jana Grill <janagrill@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#1527}
Cr-Branched-From: [f297677702651916bbf65e59c0d4bbd4ce57d1ee](https://chromium-review.googlesource.com/c/chromium/src/+2640057)-refs/heads/master@{#800218}

[modify] https://crrev.com/e75cf1792dba812a4e43a928e275f6d83df8b961/third_party/blink/renderer/core/editing/iterators/text_searcher_icu_test.cc
[modify] https://crrev.com/e75cf1792dba812a4e43a928e275f6d83df8b961/third_party/blink/renderer/core/editing/iterators/text_searcher_icu.cc

Comment 33 by janag...@google.com on Fri, Jan 22, 2021, 5:20 AM EST Project Member
Labels: -Merge-Request-86-LTS -Merge-Approved-86-LTS LTC-Merged-86

Comment 34 by [sheriffbot](#) on Tue, Jan 26, 2021, 1:53 PM EST 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

Comment 35 by amyressler@google.com on Tue, Feb 9, 2021, 9:27 AM EST Project Member
Labels: -CVE_description-missing CVE_description-submitted