Talos Vulnerability Report

TALOS-2021-1352

Google Chrome Blink setBaseAndExtent use after free vulnerability

NOVEMBER 30, 2021

CVE NUMBER

CVE-2021-30625

Summary

A use-after-free vulnerability exists in the Selection API of Blink rendering engine in Google Chrome 92.0.4515.131 (Stable) and 94.0.4597.1 (Canary). A specially-crafted web page can trigger reuse of previously freed memory which can lead to arbitrary code execution. Victim would need to visit a malicious website to trigger this vulnerability.

Tested Versions

Google Chrome 92.0.4515.131 (Stable)
Google Chrome 94.0.4597.1 (Canary)

Product URLs

https://www.google.com/chrome/

CVSSv3 Score

8.3 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L

CWE

CWE-416 - Use After Free

Details

Google Chrome is a cross-platform web browser, developed by Google.

A use-after-free vulnerability exists in Selection API in Blink, which is a main DOM parsing and rendering engine used as the core of Chromium. More specifically, the vulnerability is manifasted in implementations of the `setBaseAndExtent` method.

While executing the supplied POC, Chromium browser crashes inside `blink::LayoutObject::LayoutObjectBitfields::IsBox()` at line 17. A snippet of this function is as follows:

```
 1:  LayoutObjectBitfields(Node* node)
 2:      : self_needs_layout_for_style_(false),
 3:        self_needs_layout_for_available_space_(false),
 4:        needs_positioned_movement_layout_(false),
 5:        normal_child_needs_layout_(false),
 6:        pos_child_needs_layout_(false),
 7:        needs_simplified_normal_flow_layout_(false),
 8:        self_needs_layout_overflow_recalc_(false), {...} background_paint_location_(kBackgroundPaintInGraphicsLayer),
 9:        overflow_clip_axes_(kNoOverflowClip) {}
10:  {...}
11:  // This boolean is the cached value of 'float'
12:  // (see ComputedStyle::isFloating).
13:  ADD_BOOLEAN_BITFIELD(floating_, Floating);
14:
15:  ADD_BOOLEAN_BITFIELD(is_anonymous_, IsAnonymous);
16:  ADD_BOOLEAN_BITFIELD(is_text_, IsText);
17:  ADD_BOOLEAN_BITFIELD(is_box_, IsBox);
18:  {...}
```

The function necessary for triggering this vulnerability is “setBaseAndExtent” from the “Selection” interface, which is responsible for selecting all nodes between two nodes that are provided as arguments to the function. A prototype of this function looks like this:

`setBaseAndExtent(Node anchorNode, unsigned long anchorOffset, Node focusNode, unsigned long focusOffset);`

To trigger this vulnerability, the provided arguments must have a meaningful hierarchy: anchorNode needs to be parent to the focusNode, and parameter anchorOffset must be equal to or lower than focusOffset.

Looking down the stack trace, there is a function responsible for ComputeVisibleSelectionInDOMTree.

```
VisibleSelection SelectionEditor::ComputeVisibleSelectionInDOMTree() const {
  DCHECK_EQ(GetFrame()->GetDocument(), GetDocument());
  DCHECK_EQ(GetFrame(), GetDocument().GetFrame());
  UpdateCachedVisibleSelectionIfNeeded();
  if (cached_visible_selection_in_dom_tree_.IsNone())
    return cached_visible_selection_in_dom_tree_;
  DCHECK_EQ(cached_visible_selection_in_dom_tree_.Base().GetDocument(),
            GetDocument());
  return cached_visible_selection_in_dom_tree_;
}
```

At line 4, function UpdateCachedVisibleSelectionIfNeeded is responsible for checking if all nodes are visible. However, the statement in the style element says otherwise. It marks all nodes as “content-visibility: hidden;” which results in the engine not properly recognizing visibility of nodes inside the “DOMSelection::setBaseAndExtent” function. This leads to a use-after-free vulnerability.

With proper manipulation of node elements, this vulnerability could lead to control over freed memory and can ultimately result in remote code execution.

Crash Information

Command Line: chrome.exe –no-sandbox poc.html

```
=================================================================
==11880==ERROR: AddressSanitizer: heap-use-after-free on address 0x1200e3f5c35c at pc 0x7ff7a8b769a6 bp 0x00d9686fcba0 sp 0x00d9686fcbe8
READ of size 4 at 0x1200e3f5c35c thread T26
==11880==WARNING: Failed to use and restart external symbolizer!
[11880:9520:0804/084012.801:ERROR:service_worker_storage.cc(1899)] Failed to delete the database: Database IO error
    #0 0x7ff7a8b769a5 in blink::To<blink::LayoutBox,blink::LayoutObject>
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\platform\wtf\casting.h:127
    #1 0x7ff7ad6c018c in blink::EndsOfNodeAreVisuallyDistinctPositions
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_units.cc:530
    #2 0x7ff7ad6c1191 in blink::MostBackwardCaretPosition<blink::EditingAlgorithm<blink::FlatTreeTraversal> >
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_units.cc:669
    #3 0x7ff7ad6c060d in blink::MostBackwardOrForwardCaretPosition<blink::PositionTemplate<blink::EditingInFlatTreeStrategy> (*)(const
blink::PositionTemplate<blink::EditingInFlatTreeStrategy> &, blink::EditingBoundaryCrossingRule)>
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_units.cc:567
    #4 0x7ff7ad6b9078 in blink::CanonicalPositionOf
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_units.cc:159
    #5 0x7ff7ad6c94db in blink::VisiblePositionTemplate<blink::EditingAlgorithm<blink::NodeTraversal> >::Create
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_position.cc:121
    #6 0x7ff7ad6cbd6a in blink::CreateVisiblePosition
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_position.cc:218
    #7 0x7ff7ad57da1d in blink::VisibleSelectionTemplate<blink::EditingAlgorithm<blink::NodeTraversal> >::Creator::ComputeVisibleSelection
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_selection.cc:75
    #8 0x7ff7ad581a12 in blink::CreateVisibleSelection
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_selection.cc:100
    #9 0x7ff7ad8a1c58 in blink::SelectionEditor::UpdateCachedVisibleSelectionIfNeeded
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\selection_editor.cc:423
    #10 0x7ff7ad8a1ad0 in blink::SelectionEditor::ComputeVisibleSelectionInDOMTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\selection_editor.cc:79
    #11 0x7ff7aa5e286b in blink::FrameSelection::SetFocusedNodeIfNeeded
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\frame_selection.cc:938
    #12 0x7ff7aa5e1dd8 in blink::FrameSelection::DidSetSelectionDeprecated
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\frame_selection.cc:293
    #13 0x7ff7ad7314f6 in blink::DOMSelection::UpdateFrameSelection
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\dom_selection.cc:89
    #14 0x7ff7ad73643f in blink::DOMSelection::setBaseAndExtent
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\dom_selection.cc:385
    #15 0x7ff7b0c57b6d in blink::`anonymous namespace'::v8_selection::SetBaseAndExtentOperationCallback
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\third_party\blink\renderer\bindings\core\v8\v8_selection.cc:818
    #16 0x7ff7a4053ced in v8::internal::FunctionCallbackArguments::Call C:\b\s\w\ir\cache\builder\src\v8\src\api\api-arguments-inl.h:156
    #17 0x7ff7a4050dfd in v8::internal::`anonymous namespace'::HandleApiCallHelper<0>
C:\b\s\w\ir\cache\builder\src\v8\src\builtins\builtins-api.cc:112
    #18 0x7ff7a404e231 in v8::internal::Builtin_Impl_HandleApiCall C:\b\s\w\ir\cache\builder\src\v8\src\builtins\builtins-api.cc:142
    #19 0x7ff7a404d52e in v8::internal::Builtin_HandleApiCall C:\b\s\w\ir\cache\builder\src\v8\src\builtins\builtins-api.cc:130
    #20 0x7ee8000b81db  (<unknown module>)

0x1200e3f5c35c is located 28 bytes inside of 296-byte region [0x1200e3f5c340,0x1200e3f5c468)
freed by thread T26 here:
    #0 0x7ff7a8db642b in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82
    #1 0x7ff7ae20e62b in blink::LayoutNGTableCell::~LayoutNGTableCell
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\layout\ng\table\layout_ng_table_cell.h:18
    #2 0x7ff7aaa9d27a in blink::LayoutObject::Destroy
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\layout\layout_object.cc:3881
    #3 0x7ff7aaa9cf29 in blink::LayoutObject::DestroyAndCleanupAnonymousWrappers
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\layout\layout_object.cc:3867
    #4 0x7ff7aa55408a in blink::Node::DetachLayoutTree C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\node.cc:1726
    #5 0x7ff7aa4cb4ae in blink::Element::DetachLayoutTree C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\element.cc:2822
    #6 0x7ff7acff4b76 in blink::ContainerNode::DetachLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\container_node.cc:1015
    #7 0x7ff7aa4cb49d in blink::Element::DetachLayoutTree C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\element.cc:2819
    #8 0x7ff7aa553d0c in blink::Node::ReattachLayoutTree C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\node.cc:1690
    #9 0x7ff7aa4d446d in blink::Element::RebuildLayoutTree C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\element.cc:3175
    #10 0x7ff7acffabc1 in blink::ContainerNode::RebuildLayoutTreeForChild
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\container_node.cc:1381
    #11 0x7ff7acffaf86 in blink::ContainerNode::RebuildChildrenLayoutTrees
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\container_node.cc:1403
    #12 0x7ff7aa4d4894 in blink::Element::RebuildLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\element.cc:3203
    #13 0x7ff7ace1aa4c in blink::StyleEngine::RebuildLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\css\style_engine.cc:2076
    #14 0x7ff7ace1bf94 in blink::StyleEngine::UpdateStyleAndLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\css\style_engine.cc:2115
    #15 0x7ff7aa3ef2c2 in blink::Document::UpdateStyle C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc:2185
    #16 0x7ff7aa3ed9c2 in blink::Document::UpdateStyleAndLayoutTreeForThisDocument
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc:2134
    #17 0x7ff7aa3e41ed in blink::Document::UpdateStyleAndLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc:2054
    #18 0x7ff7aa3f0a04 in blink::Document::UpdateStyleAndLayoutTreeForNode
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc:2286
    #19 0x7ff7b05c70e7 in blink::HTMLMeterElement::CanContainRangeEndPoint
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\html\html_meter_element.cc:223
    #20 0x7ff7ad6c0178 in blink::EndsOfNodeAreVisuallyDistinctPositions
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_units.cc:529
    #21 0x7ff7ad6c1191 in blink::MostBackwardCaretPosition<blink::EditingAlgorithm<blink::FlatTreeTraversal> >
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_units.cc:669
    #22 0x7ff7ad6c060d in blink::MostBackwardOrForwardCaretPosition<blink::PositionTemplate<blink::EditingInFlatTreeStrategy> (*)(const
blink::PositionTemplate<blink::EditingInFlatTreeStrategy> &, blink::EditingBoundaryCrossingRule)>
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_units.cc:567
    #23 0x7ff7ad6b9078 in blink::CanonicalPositionOf
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_units.cc:159
    #24 0x7ff7ad6c94db in blink::VisiblePositionTemplate<blink::EditingAlgorithm<blink::NodeTraversal> >::Create
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_position.cc:121
    #25 0x7ff7ad6cbd6a in blink::CreateVisiblePosition
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_position.cc:218
    #26 0x7ff7ad57da1d in blink::VisibleSelectionTemplate<blink::EditingAlgorithm<blink::NodeTraversal> >::Creator::ComputeVisibleSelection
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_selection.cc:75
    #27 0x7ff7ad581a12 in blink::CreateVisibleSelection
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\editing\visible_selection.cc:100

previously allocated by thread T26 here:
    #0 0x7ff7a8db651b in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
    #1 0x7ff7aaa6674d in blink::LayoutObject::operator new
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\layout\layout_object.cc:237
    #2 0x7ff7adf4584c in blink::LayoutObjectFactory::CreateBlockFlow
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\layout\layout_object_factory.cc:119
    #3 0x7ff7aaa66dea in blink::LayoutObject::CreateObject
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\layout\layout_object.cc:288
    #4 0x7ff7ad4ddf4b in blink::LayoutTreeBuilderForElement::CreateLayoutObject
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\layout_tree_builder.cc:84
    #5 0x7ff7aa4c849f in blink::Element::AttachLayoutTree C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\element.cc:2729
    #6 0x7ff7acff4985 in blink::ContainerNode::AttachLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\container_node.cc:1008
    #7 0x7ff7aa4c8b4b in blink::Element::AttachLayoutTree C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\element.cc:2762
    #8 0x7ff7acff4985 in blink::ContainerNode::AttachLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\container_node.cc:1008
    #9 0x7ff7aa4c8b4b in blink::Element::AttachLayoutTree C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\element.cc:2762
    #10 0x7ff7ad557cc4 in blink::HTMLHtmlElement::AttachLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\html\html_html_element.cc:184
```

```
    #11 0x7ff7aa553d41 in blink::Node::ReattachLayoutTree C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\node.cc:1691
    #12 0x7ff7aa4d446d in blink::Element::RebuildLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\element.cc:3175
    #13 0x7ff7ace1aa4c in blink::StyleEngine::RebuildLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\css\style_engine.cc:2076
    #14 0x7ff7ace1bf94 in blink::StyleEngine::UpdateStyleAndLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\css\style_engine.cc:2115
    #15 0x7ff7aa3ef2c2 in blink::Document::UpdateStyle C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc:2185
    #16 0x7ff7aa3ed9c2 in blink::Document::UpdateStyleAndLayoutTreeForThisDocument
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc:2134
    #17 0x7ff7aa3e41ed in blink::Document::UpdateStyleAndLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc:2054
    #18 0x7ff7aa3e41dc in blink::Document::UpdateStyleAndLayoutTree
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc:2052
    #19 0x7ff7aa430c09 in blink::Document::FinishedParsing
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\dom\document.cc:6646
    #20 0x7ff7ad2a4303 in blink::HTMLDocumentParser::end
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_document_parser.cc:1422
    #21 0x7ff7ad291ae2 in blink::HTMLDocumentParser::PrepareToStopParsing
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_document_parser.cc:567
    #22 0x7ff7ad29527c in blink::HTMLDocumentParser::AttemptToEnd
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_document_parser.cc:1459
    #23 0x7ff7ad2a4a78 in blink::HTMLDocumentParser::Finish
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\html\parser\html_document_parser.cc:1522
    #24 0x7ff7ad0fbef0 in blink::DocumentLoader::FinishedLoading
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\loader\document_loader.cc:1047
    #25 0x7ff7ad103a92 in blink::DocumentLoader::StartLoadingResponse
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\loader\document_loader.cc:1631
    #26 0x7ff7ad10c35e in blink::DocumentLoader::CommitNavigation
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\loader\document_loader.cc:2370
    #27 0x7ff7acfb7188 in blink::FrameLoader::CommitDocumentLoader
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\core\loader\frame_loader.cc:1227

Thread T26 created by T0 here:
    #0 0x7ff7a8dc0c52 in __asan_wrap_CreateThread C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_win.cpp:146
    #1 0x7ff7a8fb7bae in base::`anonymous namespace'::CreateThreadInternal
C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:185
    #2 0x7ff7a8f4472a in base::Thread::StartWithOptions C:\b\s\w\ir\cache\builder\src\base\threading\thread.cc:200
    #3 0x7ff7a7d2d52f in content::RenderProcessHostImpl::Init
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_process_host_impl.cc:1967
    #4 0x7ff7a7d107b2 in content::RenderFrameHostManager::InitRenderView
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:2814
    #5 0x7ff7a7d07e1b in content::RenderFrameHostManager::ReinitializeMainRenderFrame
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:3053
    #6 0x7ff7a7d05b4e in content::RenderFrameHostManager::GetFrameHostForNavigation
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:1060
    #7 0x7ff7a7d046f6 in content::RenderFrameHostManager::DidCreateNavigationRequest
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:815
    #8 0x7ff7a7a8a579 in content::FrameTreeNode::CreatedNavigationRequest
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\frame_tree_node.cc:531
    #9 0x7ff7a7c423dd in content::Navigator::Navigate C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigator.cc:595
    #10 0x7ff7a7bb6cf3 in content::NavigationControllerImpl::NavigateWithoutEntry
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_controller_impl.cc:3302
    #11 0x7ff7a7bb5ecc in content::NavigationControllerImpl::LoadURLWithParams
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_controller_impl.cc:1136
    #12 0x7ff7aed1c47d in content::Shell::LoadURLForFrame C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell.cc:250
    #13 0x7ff7aed1c128 in content::Shell::LoadURL C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell.cc:238
    #14 0x7ff7aed1be2c in content::Shell::CreateNewWindow C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell.cc:228
    #15 0x7ff7aed6358a in content::ShellBrowserMainParts::InitializeMessageLoopContext
C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell_browser_main_parts.cc:156
    #16 0x7ff7aed63b64 in content::ShellBrowserMainParts::PreMainMessageLoopRun
C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell_browser_main_parts.cc:197
    #17 0x7ff7a725a478 in content::BrowserMainLoop::PreMainMessageLoopRun
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:949
    #18 0x7ff7a7fdb9ab in content::StartupTaskRunner::RunAllTasksNow C:\b\s\w\ir\cache\builder\src\content\browser\startup_task_runner.cc:41
    #19 0x7ff7a725997e in content::BrowserMainLoop::CreateStartupTasks
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:857
    #20 0x7ff7a72613ad in content::BrowserMainRunnerImpl::Initialize
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:131
    #21 0x7ff7a7255f90 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:43
    #22 0x7ff7a3e44814 in content::RunBrowserProcessMain C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:597
    #23 0x7ff7a3e471fd in content::ContentMainRunnerImpl::RunBrowser
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1080
    #24 0x7ff7a3e4640c in content::ContentMainRunnerImpl::Run C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:955
    #25 0x7ff7a3e43687 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:380
    #26 0x7ff7a3e43c6e in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:406
    #27 0x7ff7a0cf11d2 in main C:\b\s\w\ir\cache\builder\src\content\shell\app\shell_main.cc:33
    #28 0x7ff7b66c3093 in __scrt_common_main_seh d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #29 0x7ff8dabd7033 in BaseThreadInitThunk+0x13 (C:\Windows\System32\KERNEL32.DLL+0x180017033)
    #30 0x7ff8dc122650 in RtlUserThreadStart+0x20 (C:\Windows\SYSTEM32\ntdll.dll+0x180052650)

SUMMARY: AddressSanitizer: heap-use-after-free C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\platform\wtf\casting.h:127 in
blink::To<blink::LayoutBox,blink::LayoutObject>
Shadow bytes around the buggy address:
  0x041d006eb810: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x041d006eb820: 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa fa
  0x041d006eb830: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x041d006eb840: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x041d006eb850: fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa
=>0x041d006eb860: fa fa fa fa fa fa fa fa fd fd fd[fd]fd fd fd fd
  0x041d006eb870: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x041d006eb880: fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa
  0x041d006eb890: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x041d006eb8a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x041d006eb8b0: fd fd fd fd fd fd fd fd fd fd fd fd fd 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
==11880==ABORTING
```

Timeline

2021-08-06 - Vendor Disclosure
2021-08-24 - Vendor Patched
2021-11-30 - Public Release

CREDIT

Discovered by Marcin Towalski of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT
TALOS-2021-1364

NEXT REPORT
TALOS-2021-1384