Copy Summary | View

Closed Bug 1631618 (CVE-2020-12405) Opened 3 years ago Closed 3 years ago

[TALOS-2020-1053] use-after-free in SharedWorkerService

Categories

Product: Core
Component: DOM: Service Workers
Type: defect
Priority: P1 Severity: S2

Tracking

Status: RESOLVED FIXED
Milestone: mozilla78

Tracking Flags:

	Tracking	Status
firefox-esr68	77+	fixed
firefox76	---	wontfix
firefox77	+	fixed
firefox78	+	fixed

People (Reporter: dveditz, Assigned: edenchuang)

Details (4 keywords, Whiteboard: [post-critsmash-triage][adv-main77+][adv-esr68.9+][sec-survey])

Attachments

POC_SharedWorkerService Use-After-Free (race-condition) remote code execution.html — Details
3 years ago **Daniel Veditz [:dveditz]**
17.69 KB, text/html

testharnessreport.js — Details
3 years ago **Icewall**
13.81 KB, text/javascript

testharness-helpers.js — Details
3 years ago **Icewall**
2.10 KB, text/javascript

Bug 1631618 - Make SharedWorkerService be alive until shutdown — Details | Review
3 years ago **Eden Chuang[:edenchuang]**
47 bytes, text/x-phabricator-request
pascalc : **approval-mozilla-beta+**
RyanVM : **approval-mozilla-esr68+**
dveditz : **sec-approval+**

advisory.txt — Details
3 years ago **Frederik Braun [:freddy]**
211 bytes, text/plain

Bottom ↓ | Tags | Timeline

Daniel Veditz [:dveditz] Reporter
Description • 3 years ago

*Attached file **POC_SharedWorkerService Use-After-Free (race-condition) remote code execution.html** — Details*

[from mail to security@ from Talos, some boilerplate snipped]

Mozilla Firefox SharedWorkerService Code Execution Vulnerability

An exploitable code execution vulnerability exists in the SharedWorkerService functionality of Mozilla Firefox 76.0a1 (2020-04-01) x64. A specially crafted HTML web page can cause a use after free condition, resulting in a remote code execution. The victim needs to visit malicious web site to trigger the vulnerability.

Tested Versions

Mozilla Firefox 76.0a1 (2020-04-01) x64

CVSSv3 Score

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

CWE

CWE-416 - Use After Free

Details

Mozilla Firefox is one of the most popular web browsers on the world available for a variety of the different platforms : Windows, Linux, OSX, Android and more. Its active development ensure support for the newest web technologies like HTML5 or CSS3.

The vulnerability is related with the `SharedWorker` component and objects internaly related with it. A malicious web page can lead to a race condition situation which can cause a use-after-free vulnerability and remote code execution.

Tracking an `SharedWorkerService` object life cycle we can notice that there is an allocation made :

```
        previously allocated by thread T46 (IPDL Background) here:
                #0 0x55b699485b0d in malloc /builds/worker/fetches/llvm-project/llvm/projects/compiler-rt/lib/
                #1 0x55b6994bb4fd in moz_xmalloc /builds/worker/checkouts/gecko/memory/mozalloc/mozalloc.cpp:5
                #2 0x7fa306effc46 in operator new /builds/worker/workspace/obj-build/dist/include/mozilla/cxx
                #3 0x7fa306effc46 in mozilla::dom::SharedWorkerService::GetOrCreate() /builds/worker/checkouts
                #4 0x7fa306effa77 in mozilla::dom::SharedWorkerParent::Initialize(mozilla::dom::RemoteWorkerD
                #5 0x7fa3014c45aa in mozilla::ipc::BackgroundParentImpl::RecvPSharedWorkerConstructor(mozilla
                #6 0x7fa301c6538f in mozilla::ipc::PBackgroundParent::OnMessageReceived(IPC::Message const&) /
                #7 0x7fa30153813c in mozilla::ipc::MessageChannel::DispatchAsyncMessage(mozilla::ipc::ActorLif
                #8 0x7fa301535255 in mozilla::ipc::MessageChannel::DispatchMessage(IPC::Message&&) /builds/wor
                #9 0x7fa3015366cf in mozilla::ipc::MessageChannel::RunMessage(mozilla::ipc::MessageChannel::Me
                #10 0x7fa301536ede in mozilla::ipc::MessageChannel::MessageTask::Run() /builds/worker/checkout
                #11 0x7fa3004c58ce in nsThread::ProcessNextEvent(bool, bool*) /builds/worker/checkouts/gecko/
                #12 0x7fa3004d035c in NS_ProcessNextEvent(nsIThread*, bool) /builds/worker/checkouts/gecko/xpc
                #13 0x7fa301540ec9 in mozilla::ipc::MessagePumpForNonMainThreads::Run(base::MessagePump::Deleg
                #14 0x7fa30146cfe7 in RunInternal /builds/worker/checkouts/gecko/ipc/chromium/src/base/message
                #15 0x7fa30146cfe7 in RunHandler /builds/worker/checkouts/gecko/ipc/chromium/src/base/message_
                #16 0x7fa30146cfe7 in MessageLoop::Run() /builds/worker/checkouts/gecko/ipc/chromium/src/base/
                #17 0x7fa3004bf245 in nsThread::ThreadFunc(void*) /builds/worker/checkouts/gecko/xpcom/threads
```

Further, in a consequence of handling the next event inside another thread, the `SharedWorkerService` object gets deallocated:

```
0x606000315770 is located 48 bytes inside of 64-byte region [0x606000315740,0x606000315780)
freed by thread T0 here:
        #0 0x55b69948588d in free /builds/worker/fetches/llvm-project/llvm/projects/compiler-r
        #1 0x7fa306eff34c in operator delete /builds/worker/workspace/obj-build/dist/include/m
        #2 0x7fa306eff34c in Release /builds/worker/checkouts/gecko/dom/workers/sharedworkers/
        #3 0x7fa306eff34c in Release /builds/worker/workspace/obj-build/dist/include/mozilla/R
        #4 0x7fa306eff34c in Release /builds/worker/workspace/obj-build/dist/include/mozilla/R
        #5 0x7fa306eff34c in ~RefPtr /builds/worker/workspace/obj-build/dist/include/mozilla/R
        #6 0x7fa306eff34c in mozilla::dom::SharedWorkerManagerHolder::~SharedWorkerManagerHold
        #7 0x7fa306f04611 in mozilla::dom::SharedWorkerManagerHolder::Release() /builds/worker
        #8 0x7fa306f0853a in detail::ProxyReleaseEvent<mozilla::dom::SharedWorkerManagerHolder
        #9 0x7fa3004c58ce in nsThread::ProcessNextEvent(bool, bool*) /builds/worker/checkouts/
        #10 0x7fa3004d035c in NS_ProcessNextEvent(nsIThread*, bool) /builds/worker/checkouts/g
        #11 0x7fa30153fe6a in mozilla::ipc::MessagePump::Run(base::MessagePump::Delegate*) /bu
        #12 0x7fa30146cfe7 in RunInternal /builds/worker/checkouts/gecko/ipc/chromium/src/base
        #13 0x7fa30146cfe7 in RunHandler /builds/worker/checkouts/gecko/ipc/chromium/src/base/
        #14 0x7fa30146cfe7 in MessageLoop::Run() /builds/worker/checkouts/gecko/ipc/chromium/s
        #15 0x7fa307562ff8 in nsBaseAppShell::Run() /builds/worker/checkouts/gecko/widget/nsBa
        #16 0x7fa30aafa5bb in nsAppStartup::Run() /builds/worker/checkouts/gecko/toolkit/compo
        #17 0x7fa30ad00546 in XREMain::XRE_mainRun() /builds/worker/checkouts/gecko/toolkit/xr
        #18 0x7fa30ad023b1 in XREMain::XRE_main(int, char**, mozilla::BootstrapConfig const&)
        #19 0x7fa30ad030f3 in XRE_main(int, char**, mozilla::BootstrapConfig const&) /builds/w
        #20 0x55b6994b8726 in do_main /builds/worker/checkouts/gecko/browser/app/nsBrowserApp.
        #21 0x55b6994b8726 in main /builds/worker/checkouts/gecko/browser/app/nsBrowserApp.cpp
```

"Simultaneously" execution of thread T46 continues which in the final result leads to a use-after-free of the `SharedWorkerService` object:

```
==12981==ERROR: AddressSanitizer: heap-use-after-free on address 0x606000315770 at pc 0x7fa306f0022f b
WRITE of size 8 at 0x606000315770 thread T46 (IPDL Background)
    #0 0x7fa306f0022e in fetch_add /builds/worker/fetches/clang/bin/../lib/gcc/x86_64-unknown-linux-gn
    #1 0x7fa306f0022e in operator++ /builds/worker/workspace/obj-build/dist/include/nsISupportsImpl.h:
    #2 0x7fa306f0022e in AddRef /builds/worker/checkouts/gecko/dom/workers/sharedworkers/SharedWorkerS
    #3 0x7fa306f0022e in AddRef /builds/worker/workspace/obj-build/dist/include/mozilla/RefPtr.h:49:39
    #4 0x7fa306f0022e in AddRef /builds/worker/workspace/obj-build/dist/include/mozilla/RefPtr.h:380:3
    #5 0x7fa306f0022e in RefPtr /builds/worker/workspace/obj-build/dist/include/mozilla/RefPtr.h:109:7
    #6 0x7fa306f0022e in GetOrCreateWorkerManagerRunnable /builds/worker/checkouts/gecko/dom/workers/s
    #7 0x7fa306f0022e in mozilla::dom::SharedWorkerService::GetOrCreateWorkerManager(mozilla::dom::Sha
    #8 0x7fa306effaa7 in mozilla::dom::SharedWorkerParent::Initialize(mozilla::dom::RemoteWorkerData c
    #9 0x7fa3014c45aa in mozilla::ipc::BackgroundParentImpl::RecvPSharedWorkerConstructor(mozilla::dom
    #10 0x7fa301c6538f in mozilla::ipc::PBackgroundParent::OnMessageReceived(IPC::Message const&) /bui
    #11 0x7fa30153813c in mozilla::ipc::MessageChannel::DispatchAsyncMessage(mozilla::ipc::ActorLifecy
    #12 0x7fa301535255 in mozilla::ipc::MessageChannel::DispatchMessage(IPC::Message&&) /builds/worker
    #13 0x7fa3015366cf in mozilla::ipc::MessageChannel::RunMessage(mozilla::ipc::MessageChannel::Messa
    #14 0x7fa301536ede in mozilla::ipc::MessageChannel::MessageTask::Run() /builds/worker/checkouts/ge
    #15 0x7fa3004c58ce in nsThread::ProcessNextEvent(bool, bool*) /builds/worker/checkouts/gecko/xpcom
    #16 0x7fa3004d035c in NS_ProcessNextEvent(nsIThread*, bool) /builds/worker/checkouts/gecko/xpcom/t
    #17 0x7fa301540ed4 in mozilla::ipc::MessagePumpForNonMainThreads::Run(base::MessagePump::Delegate*
    #18 0x7fa30146cfe7 in RunInternal /builds/worker/checkouts/gecko/ipc/chromium/src/base/message_loo
    #19 0x7fa30146cfe7 in RunHandler /builds/worker/checkouts/gecko/ipc/chromium/src/base/message_loop
    #20 0x7fa30146cfe7 in MessageLoop::Run() /builds/worker/checkouts/gecko/ipc/chromium/src/base/mess
    #21 0x7fa3004bf245 in nsThread::ThreadFunc(void*) /builds/worker/checkouts/gecko/xpcom/threads/nsT
```

Further analysis revealed that the root cause of that vulnerability seems to be a lack of Mutex object in the `GetOrCreateWorkerManager` method:
https://github.com/mozilla/gecko-dev/blob/5a52cec97c41ae1eda9412dfe6f4099a9af4c7dd/dom/workers/sharedworkers/SharedWorkerService.cpp#L152

```
Line 152    void SharedWorkerService::GetOrCreateWorkerManager(
Line 153        SharedWorkerParent* aActor, const RemoteWorkerData& aData,
Line 154        uint64_t aWindowID, const MessagePortIdentifier& aPortIdentifier) {
Line 155      AssertIsOnBackgroundThread();
Line 156
Line 157      // The real check happens on main-thread.
Line 158      RefPtr<GetOrCreateWorkerManagerRunnable> r =
Line 159          new GetOrCreateWorkerManagerRunnable(this, aActor, aData, aWindowID,
Line 160                                               aPortIdentifier);
```

In `line 159` the `SharedWorkerService` object, represented by `this`, is passed as an argument to the `GetOrCreateWorkerManagerRunnable` method.
Meanwhile it is destroyed via the `~SharedWorkerManagerHolder()` destructor.

```
0x606000315770 is located 48 bytes inside of 64-byte region [0x606000315740,0x606000315780)
freed by thread T0 here:
        #0 0x55b69948588d in free /builds/worker/fetches/llvm-project/llvm/projects/compiler-rt/lib/as
        #1 0x7fa306eff34c in operator delete /builds/worker/workspace/obj-build/dist/include/mozilla/c
        #2 0x7fa306eff34c in Release /builds/worker/checkouts/gecko/dom/workers/sharedworkers/SharedWo
        #3 0x7fa306eff34c in Release /builds/worker/workspace/obj-build/dist/include/mozilla/RefPtr.h:
        #4 0x7fa306eff34c in Release /builds/worker/workspace/obj-build/dist/include/mozilla/RefPtr.h:
```

Proper heap grooming can give an attacker full control of this use-after-free vulnerability and as a result could allow it to be turned into arbitrary code execution.

Crash Information

```
=================================================================
        ==12981==ERROR: AddressSanitizer: heap-use-after-free on address 0x606000315770 at pc 0x7fa306
        WRITE of size 8 at 0x606000315770 thread T46 (IPDL Background)
                #0 0x7fa306f0022e in fetch_add /builds/worker/fetches/clang/bin/../lib/gcc/x86_64-unkn
                #1 0x7fa306f0022e in operator++ /builds/worker/workspace/obj-build/dist/include/nsISup
                #2 0x7fa306f0022e in AddRef /builds/worker/checkouts/gecko/dom/workers/sharedworkers/S
                #3 0x7fa306f0022e in AddRef /builds/worker/workspace/obj-build/dist/include/mozilla/Re
                #4 0x7fa306f0022e in AddRef /builds/worker/workspace/obj-build/dist/include/mozilla/Re
                #5 0x7fa306f0022e in RefPtr /builds/worker/workspace/obj-build/dist/include/mozilla/Re
                #6 0x7fa306f0022e in GetOrCreateWorkerManagerRunnable /builds/worker/checkouts/gecko/d
                #7 0x7fa306f0022e in mozilla::dom::SharedWorkerService::GetOrCreateWorkerManager(mozil
                #8 0x7fa306effaa7 in mozilla::dom::SharedWorkerParent::Initialize(mozilla::dom::Remote
                #9 0x7fa3014c45aa in mozilla::ipc::BackgroundParentImpl::RecvPSharedWorkerConstructor(
                #10 0x7fa301c6538f in mozilla::ipc::PBackgroundParent::OnMessageReceived(IPC::Message
                #11 0x7fa30153813c in mozilla::ipc::MessageChannel::DispatchAsyncMessage(mozilla::ipc:
                #12 0x7fa301535255 in mozilla::ipc::MessageChannel::DispatchMessage(IPC::Message&&) /b
                #13 0x7fa3015366cf in mozilla::ipc::MessageChannel::RunMessage(mozilla::ipc::MessageCh
                #14 0x7fa301536ede in mozilla::ipc::MessageChannel::MessageTask::Run() /builds/worker/
                #15 0x7fa3004c58ce in nsThread::ProcessNextEvent(bool, bool*) /builds/worker/checkouts
                #16 0x7fa3004d035c in NS_ProcessNextEvent(nsIThread*, bool) /builds/worker/checkouts/g
                #17 0x7fa301540ed4 in mozilla::ipc::MessagePumpForNonMainThreads::Run(base::MessagePum
                #18 0x7fa30146cfe7 in RunInternal /builds/worker/checkouts/gecko/ipc/chromium/src/base
                #19 0x7fa30146cfe7 in RunHandler /builds/worker/checkouts/gecko/ipc/chromium/src/base/
                #20 0x7fa30146cfe7 in MessageLoop::Run() /builds/worker/checkouts/gecko/ipc/chromium/s
```

Credit

Discovered by Marcin 'Icewall' Noga of Cisco Talos.

https://talosintelligence.com/vulnerability_reports/

Daniel Veditz [:dveditz] Reporter
Comment 1 • 3 years ago

Note: POC doesn't work, most likely because it's missing a couple of included files. Will request. Hopefully their analysis is enough to get started.

Daniel Veditz [:dveditz] Reporter
Updated • 3 years ago

Summary: [TALOS-2020-1053] Mozilla Firefox SharedWorkerService Code Execution Vulnerability → [TALOS-2020-1053] use-after-free in SharedWorkerService

Daniel Veditz [:dveditz] Reporter
Comment 2 • 3 years ago

I didn't test using an ASAN build. Maybe under ASAN the error is detected even without their memory-munging harness files.

Tyson Smith [:tsmith]
Comment 3 • 3 years ago

I am also unable to reproduce the issue with an ASan build.

Jens Stutte [:jstutte]
Comment 4 • 3 years ago

Unless we know otherwise we must assume, their exploit works. Eden, can you please give this analysis a look?

Severity: -- → critical
Flags: needinfo?(echuang)
Priority: -- → P1

Jens Stutte [:jstutte]
Comment 5 • 3 years ago

The `SharedWorkerService` is a singleton but the assumption of the comment that the `SharedWorkerParent` holds this alife long enough seems broken. The destructor already uses the sSharedWorkerMutex and nulls the pointer. As the UAF happens in `SharedWorkerService::GetOrCreateWorkerManager`, we probably do not just want to check the mutex here but need to know, that we are in the destruction phase of the `SharedWorkerService` and thus return an error.

Presumably this happens during the tear down of the process, so I think it would be hard to really exploit this (but maybe some seconds remain due to some AsyncShutdown magic).

Eden Chuang[:edenchuang] Assignee
Updated • 3 years ago

Assignee: nobody → echuang
Flags: ~~needinfo?(echuang)~~

Jason Kratzer [:jkratzer]
Comment 6 • 3 years ago

I tried to reproduce this by substituting the missing files with those from the web platform tests but was unable to do so. Dan, can you reach out to Marcin and see if he can provide us with any more details on how we might reproduce this?

Flags: needinfo?(dveditz)

Daniel Veditz [:dveditz] Reporter
Updated • 3 years ago

Flags: ~~needinfo?(dveditz)~~

Daniel Veditz [:dveditz] Reporter
Comment 7 • 3 years ago

Marcin: the testcase is missing test harness files and we cannot reproduce this crash. Can you share those with us please?

Flags: needinfo?(manoga)

Icewall
Comment 8 • 3 years ago

Attached file ***testharnessreport.js*** — *Details*

Flags: ~~needinfo?(manoga)~~

Icewall
Comment 9 • 3 years ago

Attached file ***testharness-helpers.js*** — *Details*

Icewall
Comment 10 • 3 years ago

Hi guys,
Files attached but basically these files have not been modified anyhow and come from : https://github.com/web-platform-tests/wpt/blob/master/resources/testharness.js ,etc.

Unfortunately I was not able to reproduce this bug later on after I have caught it, so its hard for me to tell anything more about it.
Information in an advisory are just my assumptions but I hope that ASAN log will tell you something more.

Eden Chuang[:edenchuang] Assignee
Comment 11 • 3 years ago

After analyzing from the stack and the codebase, the root cause might be the ~SharedWorkerService() is blocked by the lock here.

https://searchfox.org/mozilla-central/rev/41c3ea3ee8eab9ce7b82932257cb80b703cbba67/dom/workers/sharedworkers/SharedWorkerService.cpp#146

It means there is another SharedWorkerSerivce::GetOrCreate() or SharedWorkerSerivce::Get() at the same time, then ~SharedWorkerService() release the memory after these methods finishes. Then UAF happens when accessing the pointer from these methods.

The possible solution is making ~SharedWorkerService() be an atomic operation by getting the lock before entering into ~SharedWorkerService().

However, I could not reproduce the bug, could not give a proof for my guessing. But we can still apply the solution for investigation.

Daniel Veditz [:dveditz] Reporter
Updated • 3 years ago

Keywords: sec-high

Eden Chuang[:edenchuang] Assignee
Comment 12 • 3 years ago

Attached file ***Bug 1631618 - Make SharedWorkerService be alive until shutdown*** — *Details*

Jens Stutte [:jstutte]
Updated • 3 years ago

Severity: critical → S2

Phabricator Automation
Updated • 3 years ago

Attachment #9143074 - Attachment description: Bug 1631618 - Customize the AddRef() and Release() of SharedWorkerService with sSharedWorkerMutex. → Bug 1631618 - Make SharedWorkerService be alive until shutdown

Eden Chuang[:edenchuang] Assignee
Comment 13 • 3 years ago

Comment on attachment 9143074 [details]
~~Bug 1631618~~ - Make SharedWorkerService be alive until shutdown

Security Approval Request

- **How easily could an exploit be constructed based on the patch?**: Not easy, since it is not easy to contorl os thread execution in to a specific sequence.
- **Do comments in the patch, the check-in comment, or tests included in the patch paint a bulls-eye on the security problem?**: No
- **Which older supported branches are affected by this flaw?**:
- **If not all supported branches, which bug introduced the flaw?**: None
- **Do you have backports for the affected branches?**: Yes
- **If not, how different, hard to create, and risky will they be?**:
- **How likely is this patch to cause regressions; how much testing does it need?**: In basic, it should not cause any regression. All the tests should be passed with the patch.

Attachment #9143074 - Flags: sec-approval?

Daniel Veditz [:dveditz] Reporter
Updated • 3 years ago

status-firefox76: --- → wontfix
status-firefox77: --- → affected
status-firefox78: --- → affected
status-firefox-esr68: --- → affected
tracking-firefox77: --- → +
tracking-firefox78: --- → +
tracking-firefox-esr68: --- → 77+

Daniel Veditz [:dveditz] Reporter
Comment 14 • 3 years ago

Comment on attachment 9143074 [details]
~~Bug 1631618~~ - Make SharedWorkerService be alive until shutdown

sec-approval=dveditz

Attachment #9143074 - Flags: sec-approval? → sec-approval+

Cisco Talos
Comment 15 • 3 years ago

Is there a timeline for the fix/release?

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 16 • 3 years ago

https://hg.mozilla.org/integration/autoland/rev/d058127e0c10fdebb09f3902d49e14835a2f63aa

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 17 • 3 years ago

https://hg.mozilla.org/mozilla-central/rev/d058127e0c10

Group: dom-core-security → core-security-release
Status: NEW → RESOLVED
Closed: 3 years ago
status-firefox78: affected → fixed
Resolution: --- → FIXED
Target Milestone: --- → mozilla78

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 18 • 3 years ago

As this is tracking Firefox 77 and 68.9esr, please submit an uplift request.

Flags: needinfo?(echuang)

Eden Chuang[:edenchuang] Assignee
Comment 19 • 3 years ago

Comment on attachment 9143074 [details]
~~Bug 1631618~~ - Make SharedWorkerService be alive until shutdown

Beta/Release Uplift Approval Request

- **User impact if declined**: May fit UAF when browsing with SharedWorker.
- **Is this code covered by automated tests?**: Unknown
- **Has the fix been verified in Nightly?**: Yes
- **Needs manual test from QE?**: No
- **If yes, steps to reproduce**:
- **List of other uplifts needed**: None
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**: The patch is low risk. It simplifies the life cycle of SharedWorkerService and avoids maintaining the complex accessing control on a mutex.
- **String changes made/needed**:

Flags: ~~needinfo?(echuang)~~
Attachment #9143074 - Flags: approval-mozilla-beta?

Eden Chuang[:edenchuang] Assignee
Comment 20 • 3 years ago

Comment on attachment 9143074 [details]
~~Bug 1631618~~ - Make SharedWorkerService be alive until shutdown

ESR Uplift Approval Request

- **If this is not a sec:{high,crit} bug, please state case for ESR consideration**:
- **User impact if declined**: May hit UAF when browsing web with SharedWorkers
- **Fix Landed on Version**: 78
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**: The patch is low risk. It simplifies the life cycle of SharedWorkerService and avoids maintaining the complex accessing control on a mutex.
- **String or UUID changes made by this patch**:

Attachment #9143074 - Flags: approval-mozilla-esr68?

Pascal Chevrel:pascalc
Comment 21 • 3 years ago

Comment on attachment 9143074 [details]
~~Bug 1631610~~ - Make SharedWorkerService be alive until shutdown

Uplift approved for beta and esr, thanks.

Attachment #9143074 - Flags: ~~approval-mozilla-esr68?~~
Attachment #9143074 - Flags: approval-mozilla-esr68+
Attachment #9143074 - Flags: ~~approval-mozilla-beta?~~
Attachment #9143074 - Flags: approval-mozilla-beta+

Julien Cristau [:jcristau]
Comment 22 • 3 years ago

uplift

https://hg.mozilla.org/releases/mozilla-esr68/rev/dcfa7eaa9049

The patch had conflicts with ~~bug 1617993~~, hopefully the end result is fine.

status-firefox-esr68: affected → fixed

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 23 • 3 years ago

uplift

https://hg.mozilla.org/releases/mozilla-beta/rev/f482287318ff

status-firefox77: affected → fixed

Julien Cristau [:jcristau]
Comment 24 • 3 years ago

Backed out of esr68 for build failures:
https://hg.mozilla.org/releases/mozilla-esr68/rev/53e86f11003d7b8048c84d166b9b6a3beb9826c8

Example failure: https://treeherder.mozilla.org/#/jobs?repo=mozilla-esr68&revision=dcfa7eaa9049f6c177fa4f171b48eca7c44089a3&selectedTaskRun=MMfL1Aj7RX27UdhH9qgwng-0

> /builds/worker/workspace/build/src/dom/workers/sharedworkers/SharedWorkerService.cpp:168:35: error: call to non-static member function without an object argument

As far as I can tell this depends on ~~bug 1561715~~ making SchedulerGroup::Dispatch static.

status-firefox-esr68: fixed → affected
Flags: needinfo?(echuang)

Ryan VanderMeulen [:RyanVM]
Comment 25 • 3 years ago

Comment on attachment 9143074 [details]
~~Bug 1631610~~ - Make SharedWorkerService be alive until shutdown

Clearing the ESR68 approval until a rebased patch is ready.

Attachment #9143074 - Flags: ~~approval-mozilla-esr68+~~

Cornel Ionce [:noni] [Hubs QA]
Updated • 3 years ago

Flags: qe-verify-
Whiteboard: [post-critsmash-triage]

Frederik Braun [:freddy]
Updated • 3 years ago

Whiteboard: [post-critsmash-triage] → [post-critsmash-triage][adv-main77+]

Frederik Braun [:freddy]
Updated • 3 years ago

Whiteboard: [post-critsmash-triage][adv-main77+] → [post-critsmash-triage][adv-main77+][adv-esr68.9+]

Frederik Braun [:freddy]
Comment 26 • 3 years ago

(In reply to Cisco Talos from ~~comment #15~~)

> Is there a timeline for the fix/release?

While we could not reproduce the exact issue as described in your report (~~comment 6~~, ~~comment 10~~, ~~comment 11~~), we still found a likely culprit. It will be in Firefox 77 and Firefox ESR 68.9 scheduled for next Tuesday.

Frederik Braun [:freddy]
Comment 27 • 3 years ago

*Attached file **advisory.txt** — Details*

Eden Chuang[:edenchuang] Assignee
Comment 28 • 3 years ago

Comment on attachment 9143074 [details]
~~Bug 1631618~~ - Make SharedWorkerService be alive until shutdown

ESR Uplift Approval Request

- **If this is not a sec:{high,crit} bug, please state case for ESR consideration**:
- **User impact if declined**: Hit UAF on SharedWorkerService
- **Fix Landed on Version**:
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**: The patch is low risk. It simplifies the life cycle of SharedWorkerService and avoids maintaining the complex accessing control on a mutex.
- **String or UUID changes made by this patch**:

Flags: ~~needinfo?(echuang)~~
Attachment #9143074 - Flags: approval-mozilla-esr68?

Ryan VanderMeulen [:RyanVM]
Comment 29 • 3 years ago

Comment on attachment 9143074 [details]
~~Bug 1631618~~ - Make SharedWorkerService be alive until shutdown

Approved for 68.9esr. Thanks for the rebased patch!

Attachment #9143074 - Flags: approval-mozilla-esr68? → approval-mozilla-esr68+

Ryan VanderMeulen [:RyanVM]
Comment 30 • 3 years ago
uplift

https://hg.mozilla.org/releases/mozilla-esr68/rev/e17129d84f13

status-firefox-esr68: affected → fixed

Frederik Braun [:freddy]
Updated • 3 years ago

Alias: CVE-2020-12405

Release mgmt bot [:suhaib / :marco/ :calixte]
Comment 31 • 3 years ago

As part of a security bug pattern analysis, we are requesting your help with a high level analysis of this bug. It is our hope to develop static analysis (or potentially runtime/dynamic analysis) in the future to identify classes of bugs.

Please visit this google form to reply.

Flags: needinfo?(echuang)
Whiteboard: [post-critsmash-triage][adv-main77+][adv-esr68.9+] → [post-critsmash-triage][adv-main77+][adv-esr68.9+][sec-survey]

Eden Chuang[:edenchuang] Assignee
Updated • 3 years ago

Flags: ~~needinfo?(echuang)~~

Daniel Veditz [:dveditz] Reporter
Updated • 2 years ago

Group: ~~core-security-release~~

You need to log in before you can comment on or make changes to this bug.

Top ↑