Copy Summary | View

Closed Bug 1639734 (CVE-2020-12416) Opened 3 years ago Closed 3 years ago

Crash in [@ rtc::VideoBroadcaster::OnFrame]

Categories

Product: Core
Component: WebRTC
Version: 78 Branch
Platform: x86_64 Windows 10

Type: defect
Priority: P2 Severity: S3

Tracking

Status: RESOLVED FIXED
Milestone: mozilla79

Tracking Flags:	Tracking	Status
firefox-esr68	---	unaffected
firefox-esr78	78+	fixed
firefox77	---	wontfix
firefox78	+	fixed
firefox79	+	fixed

People (Reporter: alex_mayorga, Assigned: dminor)

References (Blocks 1 open bug, Regression, URL)

Details (5 keywords, Whiteboard: [post-critsmash-triage][adv-main78+][sec-survey])

Crash Data

Attachments

Bug 1639734 - Restore check that sink is registered in AddOrUpdateSink; r=bwc!
3 years ago **Dan Minor [:dminor]**
47 bytes, text/x-phabricator-request
jcristau : **approval-mozilla-beta+**
dveditz : **sec-approval+**
Details | Review

advisory.txt
3 years ago **Tom Ritter [:tjr]**
272 bytes, text/plain
Details

Bottom ↓ | Tags | Timeline

alex_mayorga Reporter
Description • 3 years ago

This bug is for crash report bp-ec8ac249-101c-4324-a463-53a880200520.

```
Top 10 frames of crashing thread:

0 xul.dll rtc::VideoBroadcaster::OnFrame media/webrtc/trunk/webrtc/media/base/videobroadcaster.cc:71
1 xul.dll mozilla::WebrtcVideoConduit::SendVideoFrame media/webrtc/signaling/src/media-conduit/VideoConduit.cp
2 xul.dll mozilla::MediaPipelineTransmit::VideoFrameFeeder::OnVideoFrameConverted media/webrtc/signaling/src/m
3 xul.dll mozilla::VideoFrameConverter::VideoFrameConverted dom/media/VideoFrameConverter.h:251
4 xul.dll mozilla::VideoFrameConverter::ProcessVideoFrame dom/media/VideoFrameConverter.h:355
5 xul.dll mozilla::detail::RunnableMethodImpl<RefPtr<mozilla::AudioTrackEncoder>, void  xpcom/threads/nsThread
6 xul.dll mozilla::TaskQueue::Runner::Run xpcom/threads/TaskQueue.cpp:212
7 xul.dll nsThreadPool::Run xpcom/threads/nsThreadPool.cpp:300
8 xul.dll nsThread::ProcessNextEvent xpcom/threads/nsThread.cpp:1211
9 xul.dll mozilla::ipc::MessagePumpForNonMainThreads::Run ipc/glue/MessagePump.cpp:332
```

¡Hola!

Crashed while on a video call on https://meet.google.com/

Filing as there are more reports over at https://crash-stats.mozilla.org/signature/?product=Firefox&signature=rtc%3A%3AVideoBroadcaster%3A%3AOnFrame

Build Configuration
Source

Built from https://hg.mozilla.org/mozilla-central/rev/8f68705097b4bf88cd61b43b14401cde98ac75b6
Build platform
target
x86_64-pc-mingw32
Build tools
Compiler Version Compiler flags
/builds/worker/fetches/clang/bin/clang-cl -Xclang -std=gnu99 10.0.0 -fcrash-diagnostics-dir=/builds/worker/artifacts -D_HAS_EXCEPTIONS=0 -W3 -Gy -Zc:inline -Gw -Wno-unknown-pragmas -Wno-ignored-pragmas -Wno-deprecated-declarations -Wno-invalid-noreturn
/builds/worker/fetches/clang/bin/clang-cl -Xclang -std=c++17 10.0.0 -Qunused-arguments -Qunused-arguments -fcrash-diagnostics-dir=/builds/worker/artifacts -TP -Zc:sizedDealloc- -D_HAS_EXCEPTIONS=0 -W3 -Gy -Zc:inline -Gw -Wno-inline-new-delete -Wno-invalid-offsetof -Wno-microsoft-enum-value -Wno-microsoft-include -Wno-unknown-pragmas -Wno-ignored-pragmas -Wno-deprecated-declarations -Wno-invalid-noreturn -Wno-inconsistent-missing-override -Wno-implicit-exception-spec-mismatch -Wno-microsoft-exception-spec -Wno-unused-local-typedef -Wno-ignored-attributes -Wno-used-but-marked-unused -D_SILENCE_TR1_NAMESPACE_DEPRECATION_WARNING -GR- -Z7 -O2 -Oy-
/builds/worker/fetches/rustc/bin/rustc 1.43.0
Configure options

MOZ_AUTOMATION=1 --target=x86_64-pc-mingw32 MOZILLA_OFFICIAL=1 --enable-update-channel=nightly MOZBUILD_STATE_PATH=/builds/worker/.mozbuild WINE=/builds/worker/fetches/wine/bin/wine64 CC=clang-cl CXX=clang-cl WINDOWSSDKDIR=/builds/worker/checkouts/gecko/vs2017_15.8.4/SDK 'DIA_SDK_PATH=/builds/worker/checkouts/gecko/vs2017_15.8.4/DIA SDK' LINKER=lld-link MAKECAB=/builds/worker/checkouts/gecko/makecab.exe NASM=/builds/worker/fetches/nasm/nasm ENABLE_CLANG_PLUGIN=1 --enable-profile-use=cross --with-pgo-profile-path=/builds/worker/fetches/merged.profdata --with-pgo-jarlog=/builds/worker/fetches/en-US.log MOZ_LTO=cross RUSTC=/builds/worker/fetches/rustc/bin/rustc CARGO=/builds/worker/fetches/rustc/bin/cargo RUSTDOC=/builds/worker/fetches/rustc/bin/rustdoc CBINDGEN=/builds/worker/fetches/cbindgen/cbindgen RUSTFMT=/builds/worker/fetches/rustc/bin/rustfmt --enable-js-shell --enable-rust-simd NODEJS=/builds/worker/fetches/node/bin/node --with-

mozilla-api-keyfile=/builds/mozilla-desktop-geoloc-api.key --with-google-location-service-api-keyfile=/builds/gls-gapi.data --with-google-safebrowsing-api-keyfile=/builds/sb-gapi.data DUMP_SYMS=/builds/worker/fetches/dump_syms/dump_syms PDBSTR=/builds/worker/fetches/pdbstr/pdbstr.exe WINCHECKSEC=/builds/worker/fetches/winchecksec/winchecksec MAKE=/usr/bin/make MAKENSISU=/builds/worker/fetches/nsis-3.01/makensis.exe UPX=/builds/worker/fetches/upx-3.95-win64/upx.exe --enable-crashreporter --with-branding=browser/branding/nightly

Please let me know if there's anything else worth collecting form this system.

¡Gracias!
Alex

Jan-Ivar Bruaroey [:jib] (needinfo? me)
Comment 1 • 3 years ago

(In reply to alex_mayorga from ~~comment #0~~)

> Filing as there are more reports over at https://crash-stats.mozilla.org/signature/?product=Firefox&signature=rtc%3A%3AVideoBroadcaster%3A%3AOnFrame

Some of those look like UAF, so I'm marking this a security bug.

Assignee: nobody → dminor
Group: media-core-security
Severity: -- → S3
Priority: -- → P2
Regressed by: ~~1622489~~

Jan-Ivar Bruaroey [:jib] (needinfo? me)
Updated • 3 years ago

No longer regressed by: ~~1622489~~

Jan-Ivar Bruaroey [:jib] (needinfo? me)
Comment 2 • 3 years ago

Byron, is this an area you're comfortable in at all, or should we wait for Dan?

Flags: needinfo?(docfaraday)

Dan Minor [:dminor] Assignee
Comment 3 • 3 years ago • Edited

I'll look into this today.

Flags: ~~needinfo?(docfaraday)~~

Daniel Veditz [:dveditz]
Updated • 3 years ago

Keywords: csectype-uaf, sec-high

Dan Minor [:dminor] Assignee
Comment 4 • 3 years ago

It looks like we're crashing here [1] with a bad sink. From a bit of testing, the only sink present is the VideoStreamEncoder created as part of the VideoSendStream here [2]. The VideoBroadcaster and VideoSendStream (and so the VideoStreamEncoder) are all managed by the VideoConduit, so my first guess is this is some sort of shutdown race when we're tearing down the VideoSendStream.

[1] https://searchfox.org/mozilla-central/rev/9aa7bebfd169bc2ead00ef596498a406e56bbb85/media/webrtc/trunk/webrtc/media/base/videobroadcaster.cc#71
[2] https://searchfox.org/mozilla-central/rev/9aa7bebfd169bc2ead00ef596498a406e56bbb85/media/webrtc/trunk/webrtc/video/video_send_stream.cc#567

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

Crash Signature: [@ rtc::VideoBroadcaster::OnFrame] → [@ rtc::VideoBroadcaster::OnFrame] [@ 0x4] [@ rtc::VideoBroadcaster::OnFrame(webrtc::VideoFrame const&)]

Dan Minor [:dminor] Assignee
Comment 6 • 3 years ago

Offhand, it looks like the RemoveSink code path should be fine. In both VideoBroadcaster::RemoveSink and VideoBroadcaster::OnFrame, the code takes the sinks_and_wants_lock_. The VideoStreamEncoder appears to block indefinitely in its Stop method before the destructor will run. I'm going to check WebrtcVideoConduit::AddOrUpdateSink next, it will dispatch to main thread if called off main thread, so perhaps we're hitting some sort of race there.

Crash Signature: [@ rtc::VideoBroadcaster::OnFrame] [@ 0x4] [@ rtc::VideoBroadcaster::OnFrame(webrtc::VideoFrame const&)] → [@ rtc::VideoBroadcaster::OnFrame] [@ 0x4] [@ rtc::VideoBroadcaster::OnFrame(webrtc::VideoFrame const&)]

Dan Minor [:dminor] Assignee
Comment 7 • 3 years ago

So I think what might be happening is that we get a call to AddOrUpdateSink off main thread, it get dispatched to main thread, but before it runs, we get a call to RemoveSink because the encoder is going way. RemoveSink succeeds, the encoder is freed, but then when AddOrUpdateSink runs, it looks like we're adding a new sink with the now invalid encoder pointer.

An earlier version of the code appears to guard against this by keeping a list of valid sinks and checking it in the dispatch code [1]. This was removed in ~~Bug 1408256~~ which I reviewed :/. That change landed in Firefox 73 and I'm not seeing any hits on crash-stats over the past year for versions older than that, other than for ESR 60, which easily could be a separate problem.

This dispatch to main is to avoid the threading assertion here [2], but VideoBroadcaster::RemoveSink takes a lock in that function anyway, so it's not clear that the assertion is really needed. We have a general problem in WebRTC where we create stuff on main and then need to access it from other threads, but the webrtc.org code assumes creation and access will all occur on a separate "worker" thread.

[1] https://searchfox.org/mozilla-central/rev/d226723e374e164b4f15d36f4b54a1a5465bd020/media/webrtc/signaling/src/media-conduit/VideoConduit.cpp#2062.
[2] https://searchfox.org/mozilla-central/rev/35b97af64a55d1d30caa4d6e9fabc1a7fbabc509/media/webrtc/trunk/webrtc/media/base/videobroadcaster.cc#37

Status: NEW → ASSIGNED

Dan Minor [:dminor] Assignee
Comment 8 • 3 years ago

Attached file ***Bug 1639734 - Restore check that sink is registered in AddOrUpdateSink; r=bwc!*** *— Details*

Dan Minor [:dminor] Assignee
Updated • 3 years ago

status-firefox77: --- → affected
status-firefox79: --- → affected
Regressed by: ~~1408256~~

BMO Automation
Updated • 3 years ago

Has Regression Range: --- → yes

Dan Minor [:dminor] Assignee
Comment 9 • 3 years ago

Comment on attachment 9155018 [details]
~~Bug 1639734~~ - Restore check that sink is registered in AddOrUpdateSink; r=bwc!

Security Approval Request

- **How easily could an exploit be constructed based on the patch?**: Not easily. Since this restores old code that was accidentally removed, I don't think it makes the underlying issue that obvious.
- **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?**: All
- **If not all supported branches, which bug introduced the flaw?**: None
- **Do you have backports for the affected branches?**: No
- **If not, how different, hard to create, and risky will they be?**: Same patch should apply cleanly to all older branches.
- **How likely is this patch to cause regressions; how much testing does it need?**: Unlikely to cause regressions, this restores old code that was accidentally removed.

Attachment #9155018 - Flags: sec-approval?

Daniel Veditz [:dveditz]
Comment 10 • 3 years ago

(In reply to Dan Minor [:dminor] from ~~comment #9~~)

> - **Which older supported branches are affected by this flaw?**: All
> - **If not all supported branches, which bug introduced the flaw?**: None

Earlier you said it was regressed by ~~bug 1408256~~ -- did that turn out to be wrong?

If ~~bug 1408256~~ is the regressor it appears that only 73 and up are affected, and if so we do not need to fix this on ESR-68 or 68-based Fennec. If the answers are really "All" and "None" then we do need an ESR backport. Please set the firefox-esr68 status flag appropriately (unaffected|affected) above.

Flags: needinfo?(dminor)

Dan Minor [:dminor] Assignee
Comment 11 • 3 years ago

(In reply to Daniel Veditz [:dveditz] from ~~comment #10~~)

> (In reply to Dan Minor [:dminor] from ~~comment #9~~)
>
> > - **Which older supported branches are affected by this flaw?**: All
> > - **If not all supported branches, which bug introduced the flaw?**: None
>
> Earlier you said it was regressed by ~~bug 1408256~~ -- did that turn out to be wrong?
>
> If ~~bug 1408256~~ is the regressor it appears that only 73 and up are affected, and if so we do not need to fix this on ESR-68 or 68-based Fennec. If the answers are really "All" and "None" then we do need an ESR backport. Please set the firefox-esr68 status flag appropriately (unaffected|affected) above.

Sorry, my bad, I was not thinking about ESR68 when I wrote that. ~~Bug 1408256~~ is the regressor and we do not need the esr68 backport.

status-firefox-esr68: --- → unaffected
Flags: ~~needinfo?(dminor)~~

Daniel Veditz [:dveditz]
Updated • 3 years ago

status-firefox-esr78: --- → affected
tracking-firefox78: --- → +
tracking-firefox79: --- → +
tracking-firefox-esr78: --- → 78+

Daniel Veditz [:dveditz]
Comment 12 • 3 years ago

Comment on attachment 9155018 [details]
~~Bug 1639734~~ - Restore check that sink is registered in AddOrUpdateSink; r=bwc!

sec-approval+

Attachment #9155018 - Flags: sec-approval? → sec-approval+

Ryan VanderMeulen [:RyanVM]
Comment 13 • 3 years ago

https://hg.mozilla.org/integration/autoland/rev/eca9af59900f33eb5774019e5b026a5f1b12bf38

Please nominate this for Beta approval when you get a chance. It grafts cleanly as-landed.

status-firefox77: affected → wontfix
Flags: needinfo?(dminor)

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 14 • 3 years ago

https://hg.mozilla.org/integration/autoland/rev/eca9af59900f33eb5774019e5b026a5f1b12bf38
https://hg.mozilla.org/mozilla-central/rev/eca9af59900f

Group: media-core-security → core-security-release
Status: ASSIGNED → RESOLVED
Closed: 3 years ago
status-firefox79: affected → fixed
Resolution: --- → FIXED
Target Milestone: --- → mozilla79

Dan Minor [:dminor] Assignee
Comment 15 • 3 years ago

Comment on attachment 9155018 [details]
~~Bug 1639734~~ - Restore check that sink is registered in AddOrUpdateSink; r=bwc!

Beta/Release Uplift Approval Request

- **User impact if declined**: Crashes / sec issues.
- **Is this code covered by automated tests?**: Yes
- **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)**: Low risk, this restores code that was accidentally removed.
- **String changes made/needed**: None

ESR Uplift Approval Request

- **If this is not a sec:{high,crit} bug, please state case for ESR consideration**: sec-high
- **User impact if declined**: Crashes / sec issues
- **Fix Landed on Version**: 79
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**: Low risk, this restores code that was accidentally removed.
- **String or UUID changes made by this patch**: None

Flags: ~~needinfo?(dminor)~~
Attachment #9155018 - Flags: approval-mozilla-esr78?
Attachment #9155018 - Flags: approval-mozilla-beta?

Julien Cristau [:jcristau]
Comment 16 • 3 years ago

Comment on attachment 9155018 [details]
~~Bug 1639734~~ - Restore check that sink is registered in AddOrUpdateSink; r=bwc!

approved for 78.0b9

Attachment #9155018 - Flags: ~~approval-mozilla-esr78?~~
Attachment #9155018 - Flags: ~~approval-mozilla-beta?~~
Attachment #9155018 - Flags: approval-mozilla-beta+

Julien Cristau [:jcristau]
Comment 17 • 3 years ago

uplift

https://hg.mozilla.org/releases/mozilla-beta/rev/d46bdc74b6c8

status-firefox78: affected → fixed
status-firefox-esr78: affected → fixed

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

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

Tom Ritter [:tjr]
Updated • 3 years ago

Whiteboard: [post-critsmash-triage] → [post-critsmash-triage][adv-main78+]

Tom Ritter [:tjr]
Comment 18 • 3 years ago

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

Release mgmt bot [:suhaib / :marco/ :calixte]
Comment 19 • 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?(dminor)
Whiteboard: [post-critsmash-triage][adv-main78+] → [post-critsmash-triage][adv-main78+][sec-survey]

Dan Minor [:dminor] Assignee
Comment 20 • 3 years ago

Done.

Flags: ~~needinfo?(dminor)~~

Tom Ritter [:tjr]
Updated • 3 years ago

Alias: CVE-2020-12416

Daniel Veditz [:dveditz]
Updated • 2 years ago

Group: ~~core-security-release~~

Marco Castelluccio [:marco]
Updated • 2 years ago

Keywords: regression

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

Top ↑