Copy Summary ▾ View ▾

Closed Bug 1643437 (CVE-2020-12420) Opened 3 years ago Closed 3 years ago

Crash in [@ nr_ice_component_process_incoming_check]

▾ **Categories**

Product: Core ▾
Component: WebRTC: Networking ▾

Type: defect
Priority: P1 Severity: S2

▾ **Tracking**

Status: RESOLVED FIXED
Milestone: mozilla79

Tracking Flags:

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

▸ **People** (Reporter: bwc, Assigned: bwc)

▸ **References**

▸ **Details** (Keywords: crash, csectype-uaf, sec-high, Whiteboard: [adv-main78+r][adv-esr68.10+r][sec-survey])

▸ **Crash Data**

▾ **Attachments**

Bug 1643437: (Copy of patch on cover bug) Make candidate pair insertion code easier to read/understand. dveditz : **sec-approval+** Details | Review
3 years ago **Byron Campen [:bwc]**
47 bytes, text/x-phabricator-request

Bottom ↓ Tags ▾ Timeline ▾

Byron Campen [:bwc] Assignee
Description • 3 years ago

This bug is for crash report bp-54620aeb-8b4a-4d7d-ac49-122e50200604.

Top 10 frames of crashing thread:

```
0 xul.dll nr_ice_component_process_incoming_check media/mtransport/third_party/nICEr/src/ice/ice_component.c:
1 xul.dll nr_ice_component_stun_server_cb media/mtransport/third_party/nICEr/src/ice/ice_component.c:1003
2 xul.dll nr_stun_server_process_request media/mtransport/third_party/nICEr/src/stun/stun_server_ctx.c:327
3 xul.dll nr_ice_socket_readable_cb media/mtransport/third_party/nICEr/src/ice/ice_socket.c:120
4 xul.dll mozilla::NrUdpSocketIpc::recv_callback_s media/mtransport/nr_socket_prsock.cpp:1594
5 xul.dll static std::_Invoker_pmf_pointer::_Call<void
6 xul.dll mozilla::runnable_args_memfn<RefPtr<mozilla::NrUdpSocketIpc>, void  media/mtransport/runnable_utils.
7 xul.dll mozilla::detail::runnable_args_base<mozilla::detail::NoResult>::Run media/mtransport/runnable_utils.
8 xul.dll nsThread::ProcessNextEvent xpcom/threads/nsThread.cpp:1211
9 xul.dll NS_ProcessNextEvent xpcom/threads/nsThreadUtils.cpp:501
```

Seems to be happening on all release channels.

Andrew McCreight [:mccr8]
Updated • 3 years ago

Keywords: csectype-uaf, sec-high

Daniel Veditz [:dveditz]
Updated • 3 years ago

Group: core-security → media-core-security

Byron Campen [:bwc] Assignee
Comment 1 • 3 years ago

It is a little hard to determine what is going on here, since it looks like the stack is not quite complete, but one possibility is that |pair| is a dangling pointer.

Byron Campen [:bwc] Assignee
Comment 2 • 3 years ago

This might be a more complete stack from esr:

https://crash-stats.mozilla.org/report/index/6bc56480-100f-4d51-97fb-d1a6a0200602

Byron Campen [:bwc] Assignee
Comment 3 • 3 years ago

So I definitely see a problem with peer (ie, remote) candidates here:

https://searchfox.org/mozilla-central/rev/598e50d2c3cd81cd616654f16af811adceb08f9f/media/mtransport/third_party/nICEr/src/ice/ice_component.c#961-969

If nr_ice_component_insert_pair fails here, the candidate pair stays in the check_list: https://searchfox.org/mozilla-central/rev/598e50d2c3cd81cd616654f16af811adceb08f9f/media/mtransport/third_party/nICEr/src/ice/ice_component.c#1712

Then, nr_ice_component_process_incoming_check will destroy the peer candidate here:

https://searchfox.org/mozilla-central/rev/598e50d2c3cd81cd616654f16af811adceb08f9f/media/mtransport/third_party/nICEr/src/ice/ice_component.c#979

This could lead to a UAF here, which is the same place we see an esr crash in ~~comment 2~~: https://searchfox.org/mozilla-central/rev/598e50d2c3cd81cd616654f16af811adceb08f9f/media/mtransport/third_party/nICEr/src/ice/ice_component.c#795

Byron Campen [:bwc] Assignee
Comment 4 • 3 years ago

Filed cover ~~bug 1644477~~.

Depends on: ~~1644477~~

Byron Campen [:bwc] Assignee
Comment 5 • 3 years ago

Attached file ***Bug 1643437: (Copy of patch on cover bug) Make candidate pair insertion code easier to read/understand.*** *— Details*

Includes removing an error code for a function that never fails, and removing
an error return when the function successfully did what it said it would.

Byron Campen [:bwc] Assignee
Comment 6 • 3 years ago

Comment on attachment 9155334 [details]
~~Bug 1643437~~: (Copy of patch on cover bug) Make candidate pair insertion code easier to read/understand.

Security Approval Request

- **How easily could an exploit be constructed based on the patch?**: Probably pretty difficult, since it does not look like a sec-bug fix.
- **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?**: Pretty easy.
- **How likely is this patch to cause regressions; how much testing does it need?**: Unlikely to cause regressions.

Attachment #9155334 - Flags: sec-approval?

Daniel Veditz [:dveditz]
Updated • 3 years ago

status-firefox77: --- → wontfix
status-firefox78: --- → affected
status-firefox79: --- → affected
status-firefox-esr68: --- → affected
tracking-firefox78: --- → +
tracking-firefox79: --- → +
tracking-firefox-esr68: --- → 78+

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

Comment on attachment 9155334 [details]
~~Bug 1643437~~: (Copy of patch on cover bug) Make candidate pair insertion code easier to read/understand.

sec-approval+

Attachment #9155334 - Flags: sec-approval? → sec-approval+

Ryan VanderMeulen [:RyanVM]
Comment 8 • 3 years ago

Looks like cover bug landed successfully. Please nominate it for Beta and ESR68 approval when you get a chance. It grafts cleanly to both as-landed.

Group: media-core-security → core-security-release
Status: NEW → RESOLVED
Closed: 3 years ago
status-firefox79: affected → fixed
status-firefox-esr78: --- → affected
tracking-firefox-esr78: --- → 78+
Flags: needinfo?(docfaraday)
Resolution: --- → FIXED
Target Milestone: --- → mozilla79

Byron Campen [:bwc] Assignee
Comment 9 • 3 years ago

Done.

Flags: ~~needinfo?(docfaraday)~~

Byron Campen [:bwc] Assignee
Comment 10 • 3 years ago • Edited

I am not sure that this is fixed just yet; we'll have to wait and see whether ~~bug 1644477~~ solved the problem.

Status: RESOLVED → REOPENED
Resolution: FIXED → ---

Release mgmt bot [:suhaib / :marco/ :calixte]
Comment 11 • 3 years ago

The patch landed in nightly and beta is affected.
:bwc, is this bug important enough to require an uplift?

If not please set `status_beta` to `wontfix`.

For more information, please visit auto_nag documentation.

Flags: needinfo?(docfaraday)

Byron Campen [:bwc] Assignee
Comment 12 • 3 years ago

Flags are being set in other bugs.

Flags: ~~needinfo?(docfaraday)~~

Julien Cristau [:jcristau]
Comment 13 • 3 years ago

Seems like we should mark this fixed.

status-firefox78: affected → fixed
status-firefox-esr68: affected → fixed
status-firefox-esr78: affected → fixed

Byron Campen [:bwc] Assignee
Comment 14 • 3 years ago

It looks like ~~bug 1644477~~ probably solved this, yes. I'm going to mark this fixed for now.

Status: REOPENED → RESOLVED
Closed: 3 years ago → 3 years ago
Resolution: --- → FIXED

Tom Ritter [:tjr]
Updated • 3 years ago

Whiteboard: [adv-main78+r]

Tom Ritter [:tjr]
Updated • 3 years ago

Whiteboard: [adv-main78+r] → [adv-main78+r][adv-esr68.10+r]

Release mgmt bot [:suhaib / :marco/ :calixte]
Comment 15 • 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?(docfaraday)
Whiteboard: [adv-main78+r][adv-esr68.10+r] → [adv-main78+r][adv-esr68.10+r][sec-survey]

Byron Campen [:bwc] Assignee
Updated • 3 years ago

Flags: ~~needinfo?(docfaraday)~~

Tom Ritter [:tjr]
Updated • 3 years ago

Alias: CVE-2020-12420

Daniel Veditz [:dveditz]
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 ↑