Starred by 3 users

Owner:	deadbeef@chromium.org **Last visit > 30 days ago**
CC:	boi...@webrtc.org janag...@google.com huib@webrtc.org orphis@chromium.org blum@chromium.org metzman@chromium.org terelius@chromium.org mea...@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>WebRTC
Modified:	Sep 15, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Deadline-Exceeded
Security_Severity-High
reward-7500
allpublic
reward-inprocess
CVE_description-submitted
Target-90
merge-merged-4240
M-91
LTR-Merged-86
LTS-Security-86
Target-91
external_security_report
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
LTS-Merged-90

Issue 1187797: Security: UAF in usrsctp on sctp_association->str_reset

Reported by korni...@gmail.com on Fri, Mar 12, 2021, 11:46 PM EST

Code

VULNERABILITY DETAILS
sctp_input.c:2097
During sctp peer restart asoc->control_send_queue is cleared and all control chunks are freed, however str_reset is not set to NULL.
This leads to UAF in `sctp_strreset_timer` (probably harmless) and `sctp_handle_stream_reset_response` (may lead to double free)

VERSION
Chrome Version: Tested on windows x64 asan build of 91.0.4441.0
Operating System: windows 10, macos, does not matter

REPRODUCTION CASE

To trigger the bug:
1. establish sctp connection
2. close a data channel -> will allocate stream_reset
3. do a sctp reconnect (RFC 4960 case A in Section 5.2.4 Table 2: XXMM (peer restarted))
4. make sure the `control_send_queue` is not empty(poc does this by sending a packet of bundled `heartbeat` and broken(wrong size) `init` chunks, this populates `control_send_queue` with `heartbeat ack` and breaks out of loop cause of broken `init` chunk)
5. next time sctp_find_stream_reset is called it may return a dangling pointer.

I've attached a poc.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: renderer
Crash State:
```
==9672==ERROR: AddressSanitizer: heap-use-after-free on address 0x1212af9904c0 at pc 0x7ffac8087eec bp 0x004217fff710 sp 0x004217fff758
READ of size 8 at 0x1212af9904c0 thread T20
    #0 0x7ffac8087eeb in sctp_find_stream_reset C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c:3859:11
    #1 0x7ffac828070c in sctp_strreset_timer C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_timer.c:1141:8
    #2 0x7ffac8070dc9 in sctp_timeout_handler C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctputil.c:2091:7
    #3 0x7ffac80aaea3 in sctp_handle_tick C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_callout.c:172:4
    #4 0x7ffac80aaff9 in user_sctp_timer_iterate C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_callout.c:214:3
    #5 0x7ffac826801f in sctp_create_thread_adapter C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_userspace.c:58:9
    #6 0x7ff76765e2b7 in __asan::AsanThread::ThreadStart(unsigned __int64) C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_thread.cpp:279
    #7 0x7ffb48967033  (C:\Windows\System32\KERNEL32.DLL+0x180017033)
    #8 0x7ffb4a7bd240  (C:\Windows\SYSTEM32\ntdll.dll+0x18004d240)

0x1212af9904c0 is located 64 bytes inside of 128-byte region [0x1212af990480,0x1212af990500)
freed by thread T17 here:
    #0 0x7ff76765441b in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82
    #1 0x7ffac80a55c1 in sctp_process_cookie_existing C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c:2106:4
    #2 0x7ffac809955f in sctp_handle_cookie_echo C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c:2957:11
```

#3 0x7ffac808e127 in sctp_process_control C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c:5457
#4 0x7ffac808e127 in sctp_common_input_processing C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c:5991:10
#5 0x7ffac7bdc679 in usrsctp_conninput C:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\user_socket.c:3342:2
#6 0x7ffac7110574 in cricket::SctpTransport::OnPacketRead(class rtc::PacketTransportInternal *, char const *, unsigned __int64, __int64 const &, int)
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\media\sctp\sctp_transport.cc:1145:5

CREDIT INFORMATION
Reporter credit: Tolyan Korniltsev

Found with fuzzing. I wonder if I could contribute my fuzzer as part of 'Chrome Fuzzer Program' ?

python_poc2.zip
251 KB Download

Comment 1 by sheriffbot on Fri, Mar 12, 2021, 11:49 PM EST Project Member

Labels: external_security_report

Comment 2 by mea...@chromium.org on Sun, Mar 14, 2021, 6:19 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: deadbeef@chromium.org
Cc: metzman@chromium.org
Labels: Security_Severity-High Security_Impact-Head OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows Pri-1
Components: Blink>WebRTC

Thanks for the report. Are you able to produce this in the latest stable version? (M89)

+deadbeef: Could you PTAL?

+metzman for the Chrome Fuzzer Program question.

Comment 3 by korni...@gmail.com on Mon, Mar 15, 2021, 4:10 AM EDT

> Are you able to produce this in the latest stable version? (M89)
Yes on 89.0.4389.90

```
(2798.4578): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
chrome_7fff2b6e0000!sctp_reset_out_streams+0x2a:
00007fff`3340800a 0fb70c6e        movzx   ecx,word ptr [rsi+rbp*2] ds:00006954`00a75000=????
0:023> k
 # Child-SP          RetAddr               Call Site
00 00000070`4edfcd20 00007fff`334076d4     chrome_7fff2b6e0000!sctp_reset_out_streams+0x2a
[c:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c @ 3801]
01 00000070`4edfcd90 00007fff`333f7767     chrome_7fff2b6e0000!sctp_handle_stream_reset_response+0x794
[c:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c @ 3942]
02 (Inline Function) --------`--------     chrome_7fff2b6e0000!sctp_handle_stream_reset+0x441
[c:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c @ 4576]
03 00000070`4edfce20 00007fff`33316a6e     chrome_7fff2b6e0000!sctp_process_control+0xcb7
[c:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c @ 5671]
04 00000070`4edfd570 00007fff`3317b051     chrome_7fff2b6e0000!sctp_common_input_processing+0x91e
[c:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\netinet\sctp_input.c @ 5998]
05 00000070`4edfd760 00007fff`3317ad70     chrome_7fff2b6e0000!usrsctp_conninput+0x191
[c:\b\s\w\ir\cache\builder\src\third_party\usrsctp\usrsctplib\usrsctplib\user_socket.c @ 3349]
06 00000070`4edfd830 00007fff`3331df92     chrome_7fff2b6e0000!cricket::SctpTransport::OnPacketRead+0x1d0
[c:\b\s\w\ir\cache\builder\src\third_party\webrtc\media\sctp\sctp_transport.cc @ 1092]
```

Comment 4 by terelius@chromium.org on Mon, Mar 15, 2021, 8:35 AM EDT Project Member

Cc: terelius@chromium.org blum@chromium.org huib@webrtc.org

Comment 5 by sheriffbot on Mon, Mar 15, 2021, 12:52 PM EDT Project Member

Labels: M-91 Target-91

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

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

Comment 6 by sheriffbot on Mon, Mar 15, 2021, 1:17 PM EDT Project Member

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 7 by deadbeef@chromium.org on Mon, Mar 15, 2021, 5:42 PM EDT Project Member

orphis@: Would you be able to take ownership on this? I'm sending an email to Tuexen.

Updating tags since this is reproducible on stable. It's possible we could get a fix in for M89 security refresh 2 (Mar 30).

Comment 8 by terelius@chromium.org on Tue, Mar 23, 2021, 5:29 AM EDT Project Member

Cc: orphis@chromium.org

Comment 9 by sheriffbot on Tue, Mar 30, 2021, 12:21 PM EDT Project Member

deadbeef: Uh oh! This issue still open and hasn't been updated in the last 14 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 10 by deadbeef@chromium.org on Tue, Mar 30, 2021, 4:20 PM EDT Project Member

No update from Michael yet, though he did say he would take a look two weeks ago.

orphis@, maybe you could take a look? It might be as simple as setting str_reset to NULL in sctp_process_cookie_existing.

Comment 11 by deadbeef@chromium.org on Tue, Mar 30, 2021, 9:24 PM EDT Project Member

Tolyan, could you provide some brief instructions on how to run the POC? Or attach a chromium debug log with verbose WebRTC logging enabled, which will dump SCTP packets with "# SCTP_PACKET" log lines?

Comment 12 by korni...@gmail.com on Tue, Mar 30, 2021, 10:18 PM EDT

deadbeef, I run it like this:
1. pip install -r requireements.txt
2. `cd web && python hello.py` to spawn a flask serving js
3. open http://127.0.0.1:5000/chrome_poc_js/index.html in a browser
4. in a separate terminal `python poc.py` # to establish rtc connection with a chrome tab and trigger the bug

I've attached filtered.log with # SCTP_PACKET dump.

filtered.log
6.0 KB View Download

Comment 13 by sheriffbot on Wed, Apr 14, 2021, 12:21 PM EDT Project Member

deadbeef: Uh oh! This issue still open and hasn't been updated in the last 14 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 deadbeef@chromium.org on Wed, Apr 14, 2021, 1:20 PM EDT Project Member

Given the information from comment #12, I created a simple usrsctp repro program which I sent to Michael Tuexen. He says he's currently working on fixing it; last update was 2 days ago.

Comment 15 by sheriffbot on Thu, Apr 15, 2021, 12:21 PM EDT Project Member

Labels: -Security_Impact-Head Security_Impact-Beta

Comment 16 by benmason@google.com on Mon, Apr 26, 2021, 11:30 AM EDT Project Member

Any further update here?

Comment 17 by deadbeef@chromium.org on Mon, Apr 26, 2021, 4:35 PM EDT Project Member

Not yet. Perhaps we should just patch this locally until the upstream fix is complete.

Comment 18 by deadbeef@chromium.org on Mon, Apr 26, 2021, 4:50 PM EDT Project Member

Actually, just a few minutes ago he committed this fix: https://github.com/sctplab/usrsctp/commit/53dd9da22a0caa77d8bcb642bcaf601b8aa6783c

Which is related to this issue but not the root cause. So maybe the actual fix is coming soon.

Comment 19 by korni...@gmail.com on Mon, May 3, 2021, 2:26 AM EDT

looks like the fix landed upstream https://github.com/sctplab/usrsctp/commit/0f8d58300b1fdcd943b4a9dd3fbd830825390d4d

Comment 20 by pbommana@google.com on Mon, May 10, 2021, 10:52 AM EDT Project Member

[Bulk Edit] Reminder M91 is already in Beta and Stable promotion is coming soon. Please review this bug and assess if this is indeed a RBS. If not, please remove the RBS label.

If so, please make sure to land the fix and request a merge into the release branch ASAP. Thank you.

Comment 21 by deadbeef@chromium.org on Mon, May 10, 2021, 3:54 PM EDT Project Member

Status: Fixed (was: Assigned)

The fix was included in this roll: https://chromium-review.googlesource.com/c/chromium/src/+/2871465

Comment 22 by deadbeef@chromium.org on Mon, May 10, 2021, 3:58 PM EDT Project Member

Labels: Merge-Request-91

Comment 23 by sheriffbot on Mon, May 10, 2021, 3:59 PM EDT Project Member

Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: M91's targeted beta branch promotion date has already passed, so this requires manual review
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 24 by deadbeef@chromium.org on Mon, May 10, 2021, 6:02 PM EDT Project Member

1. Does your merge fit within the Merge Decision Guidelines?
Yes, given that it's a severe security vulnerability.

2. Links to the CLs you are requesting to merge.

https://chromium-review.googlesource.com/c/chromium/src/+/2871465

3. Has the change landed and been verified on ToT?
Yes.

4. Does this change need to be merged into other active release branches (M-1, M+1)?
Possibly M90.

5. Why are these changes required in this milestone after branch?
Fix was not made until after branch.

6. Is this a new feature?
No.

7. If it is a new feature, is it behind a flag using finch?
N/A

Comment 25 by adetaylor@google.com on Mon, May 10, 2021, 6:05 PM EDT Project Member

Cc: mea...@chromium.org
Labels: -Merge-Review-91 Merge-Approved-91

deadbeef@ - this is a pretty big roll, but approving merge to M91, branch 4472, as this looks like it's already had 5+ days since landing and hopefully any problems would have shown up in Canary.

Please can you check the Security_Impact label here? This is currently labelled as being a bug newly introduced in M91, but that doesn't seem likely to me. meacer@ was that an assumption in #c2 or did you confirm? (It's important because of release notes credits and CVEs, which only apply for stable-affecting bugs, the fact we're blocking M91 release until we have a fix for this supposed-regression, and the (slim) chance we'd want to merge to M90).

Comment 26 by deadbeef@chromium.org on Mon, May 10, 2021, 6:30 PM EDT Project Member

Labels: -M-91 M-90

I confirmed it at least affects M90. And I suspect it goes back much further.

Comment 27 by adetaylor@chromium.org on Mon, May 10, 2021, 7:38 PM EDT Project Member

Labels: -Security_Impact-Beta -ReleaseBlock-Stable -Target-91 Security_Impact-Stable Target-90

Thanks!

In that case, Sheriffbot would have added Merge-Request-90 as well, so I'll do it.

We don't have any more planned M90 refreshes so at the moment, so I'm not going to approve M90 merge any time soon, but leaving the label here as an aide-memoire just in case.

Comment 28 by deadbeef@chromium.org on Mon, May 10, 2021, 8:29 PM EDT Project Member

I'm going to hold off on the merge for a bit because there may be a deadlock regression introduced in this range, as seen by an internal application for which usrsctp was updated at the same time.

If we don't figure it out in the next couple days, I'd say we should cherry pick just the relevant commit, as it appears to be completely self-contained:
https://chromium.googlesource.com/external/github.com/sctplab/usrsctp/+/0f8d58300b1fdcd943b4a9dd3fbd830825390d4d

Comment 29 by adetaylor@chromium.org on Mon, May 10, 2021, 11:31 PM EDT Project Member

SGTM!

Comment 30 by korni...@gmail.com on Tue, May 11, 2021, 12:45 AM EDT

deadbeef@
My fuzzer also deadlocks here ../usrsctplib/netinet/sctputil.c:1851
If I build with -DINVARIANTS it panics with "sctp_findassoc_by_vtag(): sctp_findassoc_by_vtag: tcb_mtx already locked"
I attach SCTP_DEBUG_ALL log, maybe it could be useful (I see it tries to lock a single mutex twice) .

locking_logging.txt
52.3 KB View Download

Comment 31 by sheriffbot on Tue, May 11, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 32 by sheriffbot on Tue, May 11, 2021, 1:57 PM EDT Project Member

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotifyWebRTC

Comment 33 by Git Watcher on Tue, May 11, 2021, 3:11 PM EDT Project Member

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/4b397994019194a5609680e6ec7a4e0bd22b691c

commit 4b397994019194a5609680e6ec7a4e0bd22b691c
Author: Taylor Brandstetter <deadbeef@chromium.org>
Date: Tue May 11 19:10:27 2021

[Merge M91] Roll src/third_party/usrsctp/usrsctplib/ 70d42ae95..0bd8b8110 (13 commits)

https://chromium.googlesource.com/external/github.com/sctplab/usrsctp/+log/70d42ae95a1d..0bd8b8110bc1

$ git log 70d42ae95..0bd8b8110 --date=short --no-merges --format='%ad %ae %s'
2021-05-03 yc.yang1229 Add mbedtls sha1 support (#579)
2021-05-03 tuexen Improve setup of address list for end-points
2021-05-03 tuexen Improve restart handling.
2021-05-03 tuexen Fix compilation.
2021-05-03 tuexen Improve error handling for INIT/INIT-ACK information
2021-04-30 tuexen Update vtag when scanning for INIT or INIT-ACK
2021-04-30 tuexen Handle spp_pathmtu = 0 correctly in setsockopt SCTP_PEER_ADDR_PARAMS.
2021-04-30 tuexen Use RTO.Initial of 1 sec as specified in RFC 4960bis
2021-04-30 tuexen Consistently skip chunks with incorrect length.
2021-04-28 caleb.e.allen Correct option type for UDP encapsulation port (#581)
2021-04-27 tuexen Cleanup input validation of INIT and INIT-ACK chunks
2021-04-26 tuexen Stop further processing of a packet when detecting that it contains an INIT chunk, which is too small or is not the only chunk in the packet. Still allow to finish the processing of chunks before the INIT chunk.
2021-04-26 tuexen Small cleanup, no functional change

Created with:
roll-dep src/third_party/usrsctp/usrsctplib

(cherry picked from commit 792a3a2c1b0ef87343d0102e77552d78d9715ad3)

~~Bug: chromium:1187707~~
Change-Id: I6e5fe109677f604bb12812014c10c5f86f190709
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871465
Commit-Queue: Florent Castelli <orphis@chromium.org>
Reviewed-by: Florent Castelli <orphis@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#879130}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2885634
Reviewed-by: Mirko Bonadei <mbonadei@chromium.org>
Commit-Queue: Guido Urdaneta <guidou@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#947}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/4b397994019194a5609680e6ec7a4e0bd22b691c/DEPS
[modify] https://crrev.com/4b397994019194a5609680e6ec7a4e0bd22b691c/third_party/usrsctp/README.chromium

Comment 34 by Git Watcher on Tue, May 11, 2021, 5:11 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/626c0d783d8ac8a677138d60a436e2c4b64091d7

commit 626c0d783d8ac8a677138d60a436e2c4b64091d7
Author: Taylor Brandstetter <deadbeef@chromium.org>
Date: Tue May 11 21:10:03 2021

Revert "[Merge M91] Roll src/third_party/usrsctp/usrsctplib/ 70d42ae95..0bd8b8110 (13 commits)"

This reverts commit 4b397994019194a5609680e6ec7a4e0bd22b691c.

Reason for revert: This range may have introduced a locking issue. See comments on bug.

Original change's description:
> [Merge M91] Roll src/third_party/usrsctp/usrsctplib/ 70d42ae95..0bd8b8110 (13 commits)
>
> https://chromium.googlesource.com/external/github.com/sctplab/usrsctp/+log/70d42ae95a1d..0bd8b8110bc1
>
> $ git log 70d42ae95..0bd8b8110 --date=short --no-merges --format='%ad %ae %s'
> 2021-05-03 yc.yang1229 Add mbedtls sha1 support (#579)
> 2021-05-03 tuexen Improve setup of address list for end-points
> 2021-05-03 tuexen Improve restart handling.
> 2021-05-03 tuexen Fix compilation.
> 2021-05-03 tuexen Improve error handling for INIT/INIT-ACK information
> 2021-04-30 tuexen Update vtag when scanning for INIT or INIT-ACK
> 2021-04-30 tuexen Handle spp_pathmtu = 0 correctly in setsockopt SCTP_PEER_ADDR_PARAMS.
> 2021-04-30 tuexen Use RTO.Initial of 1 sec as specified in RFC 4960bis
> 2021-04-30 tuexen Consistently skip chunks with incorrect length.
> 2021-04-28 caleb.e.allen Correct option type for UDP encapsulation port (#581)
> 2021-04-27 tuexen Cleanup input validation of INIT and INIT-ACK chunks
> 2021-04-26 tuexen Stop further processing of a packet when detecting that it contains an INIT chunk, which is too small or is not the only chunk in the packet. Still allow to finish the processing of chunks before the INIT chunk.
> 2021-04-26 tuexen Small cleanup, no functional change
>
> Created with:
>   roll-dep src/third_party/usrsctp/usrsctplib
>
> (cherry picked from commit 792a3a2c1b0ef87343d0102e77552d78d9715ad3)
>
> ~~Bug: chromium:1187707~~
> Change-Id: I6e5fe109677f604bb12812014c10c5f86f190709
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871465
> Commit-Queue: Florent Castelli <orphis@chromium.org>
> Reviewed-by: Florent Castelli <orphis@chromium.org>
> Cr-Original-Commit-Position: refs/heads/master@{#879130}
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2885634
> Reviewed-by: Mirko Bonadei <mbonadei@chromium.org>
> Commit-Queue: Guido Urdaneta <guidou@chromium.org>
> Cr-Commit-Position: refs/branch-heads/4472@{#947}
> Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

~~Bug: chromium:1187707~~
Change-Id: I72ce801cd323eeea985f3e112dc7bbb18dcfb6e5
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2888216
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Commit-Queue: Guido Urdaneta <guidou@chromium.org>
Owners-Override: Prudhvi Kumar Bommana <pbommana@google.com>
Cr-Commit-Position: refs/branch-heads/4472@{#959}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/626c0d783d8ac8a677138d60a436e2c4b64091d7/DEPS
[modify] https://crrev.com/626c0d783d8ac8a677138d60a436e2c4b64091d7/third_party/usrsctp/README.chromium

Comment 35 by deadbeef@chromium.org on Tue, May 11, 2021, 6:31 PM EDT Project Member

@ comment #30: What revision are you using specifically? sctputil.c:1851 doesn't correspond to any lock acquisition in revision 0bd8b8110 or acfce46e4.

Comment 36 by deadbeef@chromium.org on Tue, May 11, 2021, 6:43 PM EDT Project Member

Also, when you say you can reproduce it in the fuzzer, do you mean the program linked in this bug?

Comment 37 by korni...@gmail.com on Tue, May 11, 2021, 7:03 PM EDT

@ comment #35: sorry for confusion, it is https://github.com/sctplab/usrsctp/blob/acfce46e428cc084b4bd0164e1b019261a8dbeda/usrsctplib/netinet/sctputil.c#L1831
But I think it does not matter much, it could be any SCTP_TCB_LOCK macros invocation after forgotten SCTP_TCB_UNLOCK.
I did little debugging and in my repro it looks like deadlock happens when sctp_process_cookie_existing returns NULL and
https://github.com/sctplab/usrsctp/blob/acfce46e428cc084b4bd0164e1b019261a8dbeda/usrsctplib/netinet/sctp_input.c#L2933 here prevents unlocking.

I attach my repro just in case if it could help. It is a libfuzz target. To run:
cmake .. -GNinja -Dasan=off -DCMAKE_BUILD_TYPE=Debug -DCMAKE_C_COMPILER=clang -DCMAKE_CXX_COMPILER=clang++ -Dsctp_invariants=on
ninja fuzz
./usrsctplib/fuzz ../deadlock

usrsctp2.zip
2.4 MB Download

Comment 38 by mbonadei@chromium.org on Wed, May 12, 2021, 2:18 AM EDT Project Member

Cc: boi...@webrtc.org

Comment 39 by mbonadei@chromium.org on Wed, May 12, 2021, 2:34 AM EDT Project Member

Should we reopen this bug?

I am going to revert the last 2 rolls into Chromium.

Comment 40 by terelius@chromium.org on Wed, May 12, 2021, 3:39 AM EDT Project Member

Yes, I think we should reopen.

Comment 41 by terelius@chromium.org on Wed, May 12, 2021, 3:40 AM EDT Project Member

Status: Assigned (was: Fixed)

Comment 42 by korni...@gmail.com on Wed, May 12, 2021, 7:39 AM EDT

There might be same issue in process_cookie_new, Ive got another deadlock after applying 0ed173a

[usrsctp-debug] HUH? process_cookie_new: could not find INIT chunk!
[usrsctp-debug] GAK, null buffer

usrsctp3.zip
2.3 MB Download

locking_logging_cookie_new.txt
87.6 KB View Download

Comment 43 by mbonadei@chromium.org on Wed, May 12, 2021, 11:45 AM EDT Project Member

Rolling Taylor's fix (https://github.com/sctplab/usrsctp/commit/0ed173a023619cbd3466b3df4038f6fd9a541834) in Chromium: https://chromium-review.googlesource.com/c/chromium/src/+/2892204.

Comment 44 by sheriffbot on Wed, May 12, 2021, 2:07 PM EDT Project Member

Labels: Deadline-Exceeded

We commit ourselves to a 60 day deadline for fixing for high severity vulnerabilities, and have exceeded it here. If you're unable to look into this soon, could you please find another owner or remove yourself so that this gets back into the security triage queue?

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

Comment 45 by deadbeef@chromium.org on Wed, May 12, 2021, 2:13 PM EDT Project Member

FYI, the problem was introduced here: https://github.com/sctplab/usrsctp/commit/f37c12304801511a6b4e860c212cba62a2b6d962

Previously, sctp_process_cookie_existing expected the input tcb to already be locked, and returned with it still locked. But now, it sometimes calls sctp_abort_association in the error paths, which always unlocks the tcb, so the semantics were changed to "if I return NULL that means I've released the lock, otherwise I haven't", which is used in several other places. Which means the existing return NULLs needed to be updated.

This reasoning doesn't apply with sctp_process_cookie_new, unless it's being called by sctp_process_cookie_existing here (which my PR overlooked):
https://source.chromium.org/chromium/chromium/src/+/main:third_party/usrsctp/usrsctplib/usrsctplib/netinet/sctp_input.c;l=1942;drc=1776993149abe69135b509ca24e94b6c8310206b;bpv=0;bpt=1

Can you confirm whether that's what's going on? Based on the logging it definitely appears that way. Many thanks for your continued help.

Comment 46 by deadbeef@chromium.org on Wed, May 12, 2021, 2:50 PM EDT Project Member

Status: Fixed (was: Assigned)
Labels: -merge-merged-4472 -merge-merged-91 Merge-Request-91

As for what to do about this issue and M91: I'm requesting a merge again, this time to cherry pick just this usrsctp commit:
https://chromium.googlesource.com/external/github.com/sctplab/usrsctp/+/0f8d58300b1fdcd943b4a9dd3fbd830825390d4d

The alternatives would be:
* Cherry pick the entire roll again, as well as the deadlock fixes individually.
* Do a new roll that includes the deadlock fixes and cherry pick it.

But these options seem unnecessarily risky, especially when the stable cut is so soon.

Comment 47 by sheriffbot on Wed, May 12, 2021, 2:53 PM EDT Project Member

Labels: -Merge-Request-91 Merge-Review-91

This bug requires manual review: We are only 12 days from stable.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 48 by korni...@gmail.com on Wed, May 12, 2021, 3:17 PM EDT

@ comment #45:
> This reasoning doesn't apply with sctp_process_cookie_new, unless it's being called by sctp_process_cookie_existing here (which my PR overlooked):
https://source.chromium.org/chromium/chromium/src/+/main:third_party/usrsctp/usrsctplib/usrsctplib/netinet/sctp_input.c;l=1942;drc=1776993149abe69135b509ca24e94b6c8310206b;bpv=0;bpt=1 Can you confirm whether that's what's going on?

I confirm. The second deadlock happened when sctp_process_cookie_new is called from sctp_process_cookie_existing
https://github.com/sctplab/usrsctp/pull/587#issuecomment-839961754

No more deadlocks on my fuzzer corpus \M/

Comment 49 by adetaylor@google.com on Wed, May 12, 2021, 8:53 PM EDT Project Member

Labels: -Merge-Review-91 Merge-Approved-91

Approving merge to M91 for the cherry-pick in #c46.

Comment 50 by Git Watcher on Fri, May 14, 2021, 4:30 AM EDT Project Member

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/0ac2cfbe6954f19a92db6138b8b73a4fe514798e

commit 0ac2cfbe6954f19a92db6138b8b73a4fe514798e
Author: Taylor Brandstetter <deadbeef@chromium.org>
Date: Fri May 14 08:29:52 2021

Cherry picking fix for usrsctp UAF issue.

Pointing to a local usrsctp branch which has the following commit
cherry picked:
https://github.com/sctplab/usrsctp/commit/0f8d58300b1fdcd943b4a9dd3fbd830825390d4d

See log:
https://chromium.googlesource.com/external/github.com/sctplab/usrsctp/+log/70d42ae95a1d..bf12d9242a63

TBR=orphis@chromium.org

~~Bug: chromium:1187797~~
Change-Id: I0f287d255a195f52ee4e88de245d48bce9b91e2a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2893189
Commit-Queue: Florent Castelli <orphis@chromium.org>
Auto-Submit: Taylor Brandstetter <deadbeef@chromium.org>
Reviewed-by: Florent Castelli <orphis@chromium.org>
Reviewed-by: Mirko Bonadei <mbonadei@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#1045}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/0ac2cfbe6954f19a92db6138b8b73a4fe514798e/DEPS
[modify] https://crrev.com/0ac2cfbe6954f19a92db6138b8b73a4fe514798e/third_party/usrsctp/README.chromium

Comment 51 by Git Watcher on Mon, May 17, 2021, 9:24 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/168f33758e65f39849a121b7b3c292a4e30f6728

commit 168f33758e65f39849a121b7b3c292a4e30f6728
Author: Mirko Bonadei <mbonadei@chromium.org>
Date: Mon May 17 13:23:04 2021

Roll src/third_party/usrsctp/usrsctplib/ acfce46e4..22ba62ffe (3 commits)

https://chromium.googlesource.com/external/github.com/sctplab/usrsctp/+log/acfce46e428c..22ba62ffe79c

$ git log acfce46e4..22ba62ffe --date=short --no-merges --format='%ad %ae %s'
2021-05-12 tuexen Sync with FreeBSD.
2021-05-12 tuexen Improve the locking.
2021-05-12 deadbeef Unlock TCB whenever returning early from sctp_process_cookie_existing. (#587)

Created with:
roll-dep src/third_party/usrsctp/usrsctplib

~~Bug: 1187797~~
Change-Id: Ie51c9096590346c89790664bac06fad728502a1e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2891660
Commit-Queue: Mirko Bonadei <mbonadei@chromium.org>
Auto-Submit: Mirko Bonadei <mbonadei@chromium.org>
Reviewed-by: Florent Castelli <orphis@chromium.org>
Cr-Commit-Position: refs/heads/master@{#883450}

[modify] https://crrev.com/168f33758e65f39849a121b7b3c292a4e30f6728/DEPS

Comment 52 by amyressler@google.com on Thu, May 20, 2021, 1:08 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-7500

*** 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 53 by amyressler@chromium.org on Thu, May 20, 2021, 5:18 PM EDT Project Member

Congratulations, Tolyan! The VRP Panel has decided to award you $7500 for this report. Nice work!

Comment 54 by amyressler@google.com on Fri, May 21, 2021, 5:37 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 55 by amyressler@chromium.org on Mon, May 24, 2021, 11:19 AM EDT Project Member

Labels: Release-0-M91

Comment 56 by amyressler@google.com on Mon, May 24, 2021, 2:17 PM EDT Project Member

Labels: CVE-2021-30523 CVE_description-missing

Comment 57 by janag...@google.com on Tue, May 25, 2021, 10:12 AM EDT Project Member

Cc: janag...@google.com
Labels: LTS-Security-86 LTS-Merge-Request-86

Comment 58 by gianluca@google.com on Wed, May 26, 2021, 11:48 AM EDT Project Member

Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 59 by Git Watcher on Tue, Jun 1, 2021, 10:30 AM EDT Project Member

Labels: merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/eb4be47d8362e52f8c950859abacfcdc61696c9b

commit eb4be47d8362e52f8c950859abacfcdc61696c9b
Author: Taylor Brandstetter <deadbeef@chromium.org>
Date: Tue Jun 01 14:29:34 2021

[86-LTS] Cherry picking fix for usrsctp UAF issue.

Pointing to a local usrsctp branch which has the following commit
cherry picked:
https://github.com/sctplab/usrsctp/commit/0f8d58300b1fdcd943b4a9dd3fbd830825390d4d

See log:
https://chromium.googlesource.com/external/github.com/sctplab/usrsctp/+log/a6647318b57c..a0b4ea32a38c

TBR=orphis@chromium.org

(cherry picked from commit 0ac2cfbe6954f19a92db6138b8b73a4fe514798e)

~~Bug: chromium:1187707~~
Change-Id: I0f287d255a195f52ee4e88de245d48bce9b91e2a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2893189
Commit-Queue: Florent Castelli <orphis@chromium.org>
Auto-Submit: Taylor Brandstetter <deadbeef@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4472@{#1045}
Cr-Original-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2917015
Commit-Queue: Jana Grill <janagrill@google.com>
Owners-Override: Jana Grill <janagrill@google.com>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1655}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/eb4be47d8362e52f8c950859abacfcdc61696c9b/DEPS
[modify] https://crrev.com/eb4be47d8362e52f8c950859abacfcdc61696c9b/third_party/usrsctp/README.chromium

Comment 60 by janag...@google.com on Tue, Jun 1, 2021, 10:55 AM EDT Project Member

Labels: -LTS-Merge-Approved-86 LTR-Merged-86

Comment 61 by amyressler@google.com on Mon, Jun 7, 2021, 3:26 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 62 by asumaneev@google.com on Mon, Jun 7, 2021, 3:35 PM EDT Project Member

Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 63 by sheriffbot on Tue, Jun 8, 2021, 12:21 PM EDT Project Member

Labels: -M-90 M-91 Target-91

Comment 64 by gianluca@google.com on Wed, Jun 9, 2021, 10:46 AM EDT Project Member

Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 65 by Git Watcher on Wed, Jun 9, 2021, 1:14 PM EDT Project Member

Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/541dc23f0fd390e03d04bfddec1e1717cb3cfbf9

commit 541dc23f0fd390e03d04bfddec1e1717cb3cfbf9
Author: Taylor Brandstetter <deadbeef@chromium.org>
Date: Wed Jun 09 17:13:37 2021

[M90-LTS] Cherry picking fix for usrsctp UAF issue.

Pointing to a local usrsctp branch which has the following commit
cherry picked:
https://github.com/sctplab/usrsctp/commit/0f8d58300b1fdcd943b4a9dd3fbd830825390d4d

See log:
https://chromium.googlesource.com/external/github.com/sctplab/usrsctp/+log/70d42ae95a1d..bf12d9242a63

TBR=orphis@chromium.org

(cherry picked from commit 0ac2cfbe6954f19a92db6138b8b73a4fe514798e)

~~Bug: chromium:1187707~~
Change-Id: I0f287d255a195f52ee4e88de245d48bce9b91e2a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2893189
Commit-Queue: Florent Castelli <orphis@chromium.org>
Auto-Submit: Taylor Brandstetter <deadbeef@chromium.org>
Reviewed-by: Florent Castelli <orphis@chromium.org>
Reviewed-by: Mirko Bonadei <mbonadei@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4472@{#1045}
Cr-Original-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2945772
Commit-Queue: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1510}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/541dc23f0fd390e03d04bfddec1e1717cb3cfbf9/DEPS
[modify] https://crrev.com/541dc23f0fd390e03d04bfddec1e1717cb3cfbf9/third_party/usrsctp/README.chromium

Comment 66 by asumaneev@google.com on Wed, Jun 9, 2021, 1:17 PM EDT Project Member

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 67 by sheriffbot on Wed, Sep 15, 2021, 1:31 PM EDT Project Member

Labels: -Restrict-View-SecurityNotifyWebRTC 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