Starred by 3 users

Owner:	reillyg@chromium.org
CC:	adetaylor@chromium.org tsepez@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Services>Device
Modified:	Dec 16, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2020-09-09
OS:	Linux, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-10000
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
VulnerabilityAnalysis-Requested
VulnerabilityAnalysis-Submitted
Target-85
M-85
merge-merged-4183
merge-merged-85
merge-merged-4240
merge-merged-86
Release-2-M85

Issue 1121836: Security: HeapOverflow in SerialHandle

Reported by leecraso@gmail.com on Tue, Aug 25, 2020, 8:31 PM EDT

Code

VULNERABILITY DETAILS

|StartWriting|[1] could be called before the SerialPort is opened via IPC. The pending-check will be done in |OnFileCanWriteWithoutBlocking|[2]. But before that, the illegal fd(-1) could be passed into |WatchWritable|[3]. Eventually cause heap overflow at [4].

```
    ...

    evep = &epollop->fds[fd];  //<<<----------
    op = EPOLL_CTL_ADD;
    events = 0;
    if (evep->evread != NULL) {
        events |= EPOLLIN;
        op = EPOLL_CTL_MOD;
    }
    if (evep->evwrite != NULL) {
        events |= EPOLLOUT;
        op = EPOLL_CTL_MOD;
    }
    ...

    if (ev->ev_events & EV_READ)
        evep->evread = ev;
    if (ev->ev_events & EV_WRITE)
        evep->evwrite = ev;
```

[1]. https://source.chromium.org/chromium/chromium/src/+/master:services/device/public/mojom/serial.mojom;l=167;drc=97254d4f8844ae362125e62aee4b209c5fc67534;bpv=1;bpt=0?originalUrl=https:%2F%2Fcs.chromium.org%2F
[2]. https://source.chromium.org/chromium/chromium/src/+/master:services/device/serial/serial_io_handler_posix.cc;l=373;drc=4a991b979bb82defc403bba68c87405bf01ea70c;bpv=1;bpt=0?originalUrl=https:%2F%2Fcs.chromium.org%2F
[3]. https://source.chromium.org/chromium/chromium/src/+/master:services/device/serial/serial_io_handler_posix.cc;l=410;drc=4a991b979bb82defc403bba68c87405bf01ea70c;bpv=1;bpt=0?originalUrl=https:%2F%2Fcs.chromium.org%2F
[4]. https://source.chromium.org/chromium/chromium/src/+/master:base/third_party/libevent/epoll.c;l=280;drc=c7ebe6daa79da2e351345065020cc7f216126f15;bpv=1;bpt=0?originalUrl=https:%2F%2Fcs.chromium.org%2F

VERSION

Chrome Version: M85 stable
Operating System: Linux

REPRODUCTION CASE
1. Apply the attached token.patch(*).
2. $ python ./copy_mojo_js_bindings.py /path/to/chrome/.../out/asan/gen
   $ python -m SimpleHTTPServer

   $ out/asan/chrome --enable-blink-features=MojoJS --user-data-dir=/tmp/xxxx "http://localhost:8000/poc.html"
3. Select any serial device and click the triggerButton.

* ps: Similar to https://bugs.chromium.org/p/chromium/issues/detail?id=998548, the token.patch aims to solve a javascript bug in the mojo API mojoBinding.js, it has nothing to do with the vulnerability itself. This can be fixed from the renderer side or by using the cpp API.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: browser
Crash State: see asan file

CREDIT INFORMATION
Reporter credit: Leecraso and Guang Gong of 360 Alpha Lab working with 360 BugCloud

asan
15.3 KB View Download

token.patch
679 bytes View Download

poc.html
1.0 KB View Download

Comment 1 by tsepez@chromium.org on Wed, Aug 26, 2020, 11:43 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: reillyg@chromium.org
Labels: Security_Impact-Stable Security_Severity-High OS-Chrome OS-Linux OS-Mac
Components: Internals>Services>Device

reillyg - could you take a look? It looks like you've done some work in the past in this area with closed fds, or feel free to re-assign as appropriate. Thanks!

Comment 2 by sheriffbot on Wed, Aug 26, 2020, 2:04 PM EDT Project Member

Labels: Target-85 M-85

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 3 by sheriffbot on Wed, Aug 26, 2020, 2:45 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 4 by rsesek@chromium.org on Thu, Sep 3, 2020, 11:57 AM EDT Project Member

reillyg: Friendly ping. This is a high-severity vulnerability affecting stable.

Comment 5 by reillyg@chromium.org on Thu, Sep 3, 2020, 2:32 PM EDT Project Member

Sorry, I haven't been able to get to this because of Perf. I will have a fix today.

Comment 6 by reillyg@chromium.org on Thu, Sep 3, 2020, 3:56 PM EDT Project Member

Status: Started (was: Assigned)

A fix is out for review: https://chromium-review.googlesource.com/c/chromium/src/+/2393001

I have a more holistic fix planned as part of resolving ~~issue 1121774~~ but this is the minimal mergeable version.

Comment 7 by bugdroid on Tue, Sep 8, 2020, 3:30 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/adc731d678c4c795e7c4c74133a624310e7bc9ae

commit adc731d678c4c795e7c4c74133a624310e7bc9ae
Author: Reilly Grant <reillyg@chromium.org>
Date: Tue Sep 08 19:29:40 2020

serial: Check that port is open before reading or writing

This change adds checks to the platform-specific implementations
of Read() and Write() to make sure that the file descriptor is
valid before. This makes the assumptions validated by later DCHECK
correct.

This cannot be done in the platform-independent layer because test
code depends on being able to call some SerialIoHandler methods
without an actual file descriptor.

~~Bug: 1121936~~
Change-Id: If182404cf10a2f3b445b9c80b75fed5df6b5ab4b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2393001
Reviewed-by: James Hollyer <jameshollyer@chromium.org>
Commit-Queue: Reilly Grant <reillyg@chromium.org>
Cr-Commit-Position: refs/heads/master@{#805016}

[modify] https://crrev.com/adc731d678c4c795e7c4c74133a624310e7bc9ae/services/device/serial/serial_io_handler_posix.cc
[modify] https://crrev.com/adc731d678c4c795e7c4c74133a624310e7bc9ae/services/device/serial/serial_io_handler_win.cc
[modify] https://crrev.com/adc731d678c4c795e7c4c74133a624310e7bc9ae/services/device/serial/serial_port_impl_unittest.cc

Comment 8 by reillyg@chromium.org on Tue, Sep 8, 2020, 3:47 PM EDT Project Member

Status: Fixed (was: Started)
Cc: tsepez@chromium.org
NextAction: 2020-09-09

Marking this issue fixed. I will request a merge to M-86 after validating the fix is stable on canary-channel tomorrow.

tsepez@, do you think this should be merged to M-86?

Comment 9 by sheriffbot on Wed, Sep 9, 2020, 3:09 PM EDT Project Member

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

Comment 10 by sheriffbot on Wed, Sep 9, 2020, 3:29 PM EDT Project Member

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

Requesting merge to stable M85 because latest trunk commit (805016) appears to be after stable branch point (782793).

Requesting merge to beta M86 because latest trunk commit (805016) appears to be after beta branch point (800218).

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

Comment 11 by sheriffbot on Wed, Sep 9, 2020, 3:35 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 12 by reillyg@chromium.org on Wed, Sep 9, 2020, 6:15 PM EDT Project Member

1. Does your merge fit within the Merge Decision Guidelines?
Yes.

2. Links to the CLs you are requesting to merge.
https://chromium-review.googlesource.com/c/chromium/src/+/2393001

3. Has the change landed and been verified on master/ToT?
Yes, I have validated the change on macOS and Windows with Chrome Canary.

4. Why are these changes required in this milestone after branch?
This is a Security_Severity-High issue which affects the M-86 branch.

5. Is this a new feature?
No.

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

Comment 13 by srinivassista@google.com on Wed, Sep 9, 2020, 7:26 PM EDT Project Member

Cc: adetaylor@chromium.org

reillyg@ does this need to be merged to M85 now? or can this wait for M86

+adetaylor@

Comment 14 by reillyg@chromium.org on Wed, Sep 9, 2020, 8:04 PM EDT Project Member

According to the severity guidelines[1] a high-severity issue this should be merged into the current stable milestone.

[1] https://chromium.googlesource.com/chromium/src/+/master/docs/security/severity-guidelines.md

Comment 15 by adetaylor@chromium.org on Thu, Sep 10, 2020, 11:52 AM EDT Project Member

Labels: -Merge-Request-85 -Merge-Review-86 Merge-Approved-85 Merge-Approved-86

Yes, I think this is sufficiently simple that we should follow the merge guidelines as normal. Approving merge to M86 (branch 4240) and M85 (branch 4183). We'll likely release this with the final M85 stable security refresh in about 10 days.

reillyg@ please wait for a day of canary coverage before merging anywhere.

Comment 16 by bugdroid on Fri, Sep 11, 2020, 7:31 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/+/e07e479165fc1237e42c755a9f77585affa5bf24

commit e07e479165fc1237e42c755a9f77585affa5bf24
Author: Reilly Grant <reillyg@chromium.org>
Date: Fri Sep 11 23:28:19 2020

serial: Check that port is open before reading or writing

This change adds checks to the platform-specific implementations
of Read() and Write() to make sure that the file descriptor is
valid before. This makes the assumptions validated by later DCHECK
correct.

This cannot be done in the platform-independent layer because test
code depends on being able to call some SerialIoHandler methods
without an actual file descriptor.

(cherry picked from commit adc731d678c4c795e7c4c74133a624310e7bc9ae)

~~Bug: 1121836~~
Change-Id: If182404cf10a2f3b445b9c80b75fed5df6b5ab4b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2393001
Reviewed-by: James Hollyer <jameshollyer@chromium.org>
Commit-Queue: Reilly Grant <reillyg@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#805016}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2406664

Reviewed-by: Reilly Grant <reillyg@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#632}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/e07e479165fc1237e42c755a9f77585affa5bf24/services/device/serial/serial_io_handler_posix.cc
[modify] https://crrev.com/e07e479165fc1237e42c755a9f77585affa5bf24/services/device/serial/serial_io_handler_win.cc
[modify] https://crrev.com/e07e479165fc1237e42c755a9f77585affa5bf24/services/device/serial/serial_port_impl_unittest.cc

Comment 17 by bugdroid on Fri, Sep 11, 2020, 10:32 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/+/21069131d16de0a2e649cf0cb38860f1bbc8ccff

commit 21069131d16de0a2e649cf0cb38860f1bbc8ccff
Author: Reilly Grant <reillyg@chromium.org>
Date: Sat Sep 12 02:30:46 2020

serial: Check that port is open before reading or writing

This change adds checks to the platform-specific implementations
of Read() and Write() to make sure that the file descriptor is
valid before. This makes the assumptions validated by later DCHECK
correct.

This cannot be done in the platform-independent layer because test
code depends on being able to call some SerialIoHandler methods
without an actual file descriptor.

(cherry picked from commit adc731d678c4c795e7c4c74133a624310e7bc9ae)

(cherry picked from commit e07e479165fc1237e42c755a9f77585affa5bf24)

~~Bug: 1121836~~
Change-Id: If182404cf10a2f3b445b9c80b75fed5df6b5ab4b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2393001
Reviewed-by: James Hollyer <jameshollyer@chromium.org>
Commit-Queue: Reilly Grant <reillyg@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#805016}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2406664
Reviewed-by: Reilly Grant <reillyg@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4240@{#632}
Cr-Original-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2406151
Cr-Commit-Position: refs/branch-heads/4183@{#1813}
Cr-Branched-From: 740e9e8a40505392ba5c8e022a8024b3d018ca65-refs/heads/master@{#782793}

[modify] https://crrev.com/21069131d16de0a2e649cf0cb38860f1bbc8ccff/services/device/serial/serial_io_handler_posix.cc
[modify] https://crrev.com/21069131d16de0a2e649cf0cb38860f1bbc8ccff/services/device/serial/serial_io_handler_win.cc
[modify] https://crrev.com/21069131d16de0a2e649cf0cb38860f1bbc8ccff/services/device/serial/serial_port_impl_unittest.cc

Comment 18 by adetaylor@google.com on Mon, Sep 14, 2020, 2:31 PM EDT Project Member

Labels: reward-topanel

Comment 19 by adetaylor@google.com on Wed, Sep 16, 2020, 7:15 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-10000

*** 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 20 by adetaylor@google.com on Wed, Sep 16, 2020, 7:18 PM EDT Project Member

Congratulations! The VRP panel has decided to award $10,000 for this report.

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

Labels: Release-2-M85

Comment 22 by adetaylor@google.com on Thu, Sep 24, 2020, 1:36 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 23 by mmoroz@chromium.org on Tue, Sep 29, 2020, 2:19 PM EDT Project Member

Labels: VulnerabilityAnalysis-Requested

reillyg@, thank you for fixing this issue. Chrome Security team needs your knowledge to prevent that whole class of bugs from happening elsewhere. We would greatly appreciate if you could tell us more about the issue by filling out the following form: https://forms.gle/VWKDUv9a8GXCCRWm7

Comment 24 by mmoroz@chromium.org on Wed, Oct 7, 2020, 6:53 PM EDT Project Member

Labels: VulnerabilityAnalysis-Submitted

Comment 25 by sheriffbot on Wed, Dec 16, 2020, 1:51 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