Starred by 4 users

**Owner:** mthiesse@chromium.org

**CC:** rsesek@chromium.org
yfrie...@chromium.org
ejc@google.com
mthiesse@chromium.org
majidvp@chromium.org
yigu@chromium.org

**Status:** Fixed *(Closed)*

**Components:** Blink>WebOTP

**Modified:** Jul 29, 2022

**Backlog-Rank:** ----

**Editors:** ----

**EstimatedDays:** ----

**NextAction:** ----

**OS:** Android

**Pri:** 2

**Type:** Bug-Security

Reward-1000
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
FoundIn-83
external_security_report
external_security_bug
Security_Impact-Extended
Release-0-M100
CVE-2022-1130

# Issue 1142269: Security: Chromium doesn't conform to SMS Verification APIs leading to potential Access to app protected components vulnerability

Reported by secur...@oversecured.com on Sun, Oct 25, 2020, 12:48 PM EDT

Code

Hey, I scanned multiple apps internally using Oversecured scanner and noticed that the most of them doesn't conform to official guidelines https://developers.google.com/identity/sms-retriever/user-consent/request#2_start_listening_for_incoming_messages

The guidelines require to ask the broadcast sender to have SmsRetriever.SEND_PERMISSION. However it's registered without any required permissions:
https://chromium.googlesource.com/chromium/src/+/refs/heads/master/content/public/android/java/src/org/chromium/content/browser/sms/SmsUserConsentReceiver.java#60

It may lead to Access to app protected components vulnerability (https://oversecured.com/vulnerabilities#Ability_to_start_arbitrary_components).

I tried to reproduce this issue in Google Chrome on Samsung Galaxy S8 Android 7.0 and an Emulator with Android 10. Chrome on the device crashes with NullPointerException (on this line https://chromium.googlesource.com/chromium/src/+/refs/heads/master/content/public/android/java/src/org/chromium/content/browser/sms/SmsUserConsentReceiver.java#108), because `mWindowAndroid` is null (`SmsUserConsentReceiver.listen(WindowAndroid)` is never called). And nothing happens on the emulator.

The received intent in `SmsRetriever.EXTRA_CONSENT_INTENT` is launched then without any security checks in the app's context (e.g. in Google Chrome). I'd like to bring your attention to this issue.

Thanks,
Sergey Toshin
Oversecured Inc.

Comment 1 by ochang@google.com on Sun, Oct 25, 2020, 8:12 PM EDT Project Member

**Status:** Assigned (was: Unconfirmed)
**Owner:** goto@chromium.org
**Labels:** Security_Severity-Low Security_Impact-Stable OS-Android
**Components:** Blink>WebOTP

goto, could you please take a look at this?

Comment 2 by sheriffbot on Mon, Oct 26, 2020, 1:42 PM EDT Project Member

**Labels:** -Pri-3 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 3 by sheriffbot on Fri, Oct 30, 2020, 6:45 PM EDT Project Member

**Labels:** reward-potential

Comment 4 by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST Project Member

**Labels:** -reward-potential external_security_report

Comment 5 by sheriffbot on Wed, Mar 10, 2021, 8:04 PM EST Project Member

**Labels:** reward-potential

Comment 6 by zhangtiff@google.com on Wed, Mar 17, 2021, 7:12 PM EDT Project Member

**Labels:** -reward-potential external_security_bug

Comment 7 by xinghuilu@chromium.org on Thu, Feb 3, 2022, 3:09 AM EST Project Member

**Cc:** majidvp@chromium.org ayui@chromium.org rsesek@chromium.org mthiesse@chromium.org yfrie...@chromium.org

~~Issue 1293506~~ has been merged into this issue.

Comment 8 by xinghuilu@chromium.org on Thu, Feb 3, 2022, 3:11 AM EST Project Member

**Status:** Started (was: Assigned)
**Owner:** mthiesse@chromium.org
**Labels:** -Security_Severity-Low -Security_Impact-Stable FoundIn-83 Security_Severity-High

Raising severity to high because it allows any app on the device to send arbitrary intents to non-exported components within Chrome.

Comment 9 by sheriffbot on Thu, Feb 3, 2022, 3:12 AM EST Project Member

**Labels:** Security_Impact-Extended

Comment 10 by Git Watcher on Thu, Feb 3, 2022, 5:24 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc

commit f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc
Author: Michael Thiessen <mthiesse@chromium.org>
Date: Thu Feb 03 22:23:06 2022

Check Broadcast permissions in SmsUserConsentReceiver

In order to avoid any app sending us an
SmsRetriever.SMS_RETRIEVED_ACTION broadcast, we need to check that the
sender has the SmsRetriever.SEND_PERMISSION permission. This permission
ensures that only Google Play Services can send the broadcast.

The unit tests were also failing when run locally due to
LifetimeAssertions in Java because the WindowAndroid wasn't being
destroyed correctly, so I fixed it in all of the unit tests that create
WindowAndroids from c++.

~~Bug: 1142269~~

Change-Id: I3278919c566e1fc344ed0f4adce74fbf93a85c53
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3434025
Reviewed-by: Yi Gu <yigu@chromium.org>

Reviewed-by: Yi Gu <yigu@chromium.org>
Commit-Queue: Michael Thiessen <mthiesse@chromium.org>
Auto-Submit: Michael Thiessen <mthiesse@chromium.org>
Reviewed-by: Bo Liu <boliu@chromium.org>
Commit-Queue: Bo Liu <boliu@chromium.org>
Cr-Commit-Position: refs/heads/main@{#966953}

[modify] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/content/public/android/java/src/org/chromium/content/browser/sms/SmsUserConsentReceiver.java
[modify] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/ui/android/resources/resource_manager_impl_unittest.cc
[modify] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/content/public/android/java/src/org/chromium/content/browser/sms/Wrappers.java
[modify] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/ui/android/BUILD.gn
[modify] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/ui/android/java/src/org/chromium/ui/base/WindowAndroid.java
[rename] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/ui/android/view_android_unittest.cc
[modify] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/ui/android/window_android.cc
[modify] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/ui/android/window_android.h
[modify] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/content/browser/sms/sms_provider_gms_unittest.cc
[modify] https://crrev.com/f42f9f333a4e0f8c69f9d8c1e2bd52f08897b2bc/content/browser/renderer_host/render_widget_host_view_android_unittest.cc

Comment 11 by mthiesse@chromium.org on Thu, Feb 3, 2022, 5:53 PM EST Project Member

**Status:** Fixed (was: Started)

Comment 12 by mthiesse@chromium.org on Fri, Feb 4, 2022, 10:23 AM EST Project Member

**Cc:** ejc@google.com

Comment 13 by sheriffbot on Fri, Feb 4, 2022, 12:41 PM EST Project Member

**Labels:** reward-topanel

Comment 14 by sheriffbot on Sat, Feb 5, 2022, 1:40 PM EST Project Member

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

Comment 15 by amyressler@google.com on Thu, Feb 17, 2022, 6:34 PM EST Project Member

**Labels:** -reward-topanel reward-unpaid reward-1000

*** 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

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 16 by amyressler@chromium.org on Thu, Feb 17, 2022, 6:37 PM EST Project Member

Hello, thank you for this report. The Chrome VRP would like to extend a $1000 reward to thank you for taking this time to report this issue to us. A member of our finance team will be in touch soon to arrange payment.

Comment 17 by amyressler@google.com on Fri, Feb 18, 2022, 3:01 PM EST Project Member

**Labels:** -reward-unpaid reward-inprocess

Comment 18 by amyressler@chromium.org on Mon, Mar 28, 2022, 6:37 PM EDT Project Member

**Labels:** Release-0-M100

Comment 19 by amyressler@google.com on Tue, Mar 29, 2022, 1:13 PM EDT Project Member

**Labels:** CVE-2022-1130 CVE_description-missing

Comment 20 by ayui@chromium.org on Tue, Mar 29, 2022, 1:14 PM EDT Project Member

**Cc:** -ayui@chromium.org

Comment 21 by sheriffbot on Fri, May 13, 2022, 1:32 PM EDT 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

Comment 22 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

**Labels:** CVE_description-submitted -CVE_description-missing

Comment 23 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:27 PM EDT Project Member

**Labels:** -CVE_description-missing --CVE_description-missing