Starred by 2 users

Owner:	rdevl...@chromium.org
CC:	fsam...@chromium.org rdevl...@chromium.org solomonkinard@chromium.org tjudkins@chromium.org
Status:	Fixed *(Closed)*
Components:	Platform>Extensions>API
Modified:	Apr 14, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac
Pri:	2
Type:	Bug-Security

reward-500
Security_Severity-Low
Security_Impact-Stable
allpublic
reward-inprocess
CVE_description-submitted
Target-77
Target-78
Target-79
M-79
Release-0-M81
CVE-2020-6438

Issue 714617: Security: chrome.tabs.executeScript can reveal Chrome's profile path

Reported by ngy...@gmail.com on Mon, Apr 24, 2017, 10:00 AM 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://www.chromium.org/Home/chromium-security/security-faq

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

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

VULNERABILITY DETAILS

VERSION
Chrome Version: 58.0.3029.81 stable, 60.0.3079.0 canary
Operating System: Windows 7 SP1, also reproducible on macOS 10.12.4

REPRODUCTION CASE
1. Install the attached extension
2. Go to http://example.com
3. Read the error message

Expected result:
The JavaScript error stack should only show `executed.js` or something like `chrome-extension://dogncidbhigdogloimjmnldclfogpmin/executed.js`

Actual result:
The JavaScript error stack is revealing Chrome's profile path, which most likely contains the OS username too

```
Error
    at file:///C:/Users/ngyikp/AppData/Local/Google/Chrome/User%20Data/Default/Extensions/dogncidbhigdogloimjmnldclfogpmin/1.0_0/executed.js:2:8
```

Source code:
content.js:
```
chrome.runtime.sendMessage('', function() {});
```

background.js:
```
chrome.runtime.onMessage.addListener(function(message, sender, callback) {
	chrome.tabs.executeScript(sender.tab.id, {file: 'executed.js'});
});
```

executed.js:
```
try {
	throw new Error();
} catch (ex) {
	alert(ex.stack);
}
```

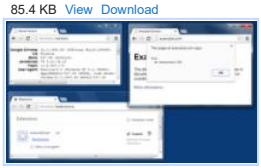
manifest.json:
```
{
	"name": "executeScript",
	"version": "1.0",

	"background": {
		"scripts": ["background.js"],
		"persistent": false
	},
	"manifest_version": 2,

	"permissions": [
		"http://example.com/*",
		"https://example.com/*",
		"http://www.example.com/*",
		"https://www.example.com/*"
	],
	"content_scripts": [{
		"include_globs": [
			"http://example.com/*",
			"https://example.com/*",
			"http://www.example.com/*",
			"https://www.example.com/*"
		],
		"js": ["content.js"],
		"matches": [
			"http://example.com/*",
			"https://example.com/*",
			"http://www.example.com/*",
			"https://www.example.com/*"
		],
		"run_at": "document_start"
	}]
}
```

This bug is introduced since Chrome 32, Chrome 31 is OK

This commit seems suspect: https://chromium.googlesource.com/chromium/src/+/a7074d1c5c07670813eefdbf286c23416e528123%5E%21/

screenshot.png
71.4 KB View Download

chrome31.png
85.4 KB View Download



Comment 1 by ngy...@gmail.com on Mon, Apr 24, 2017, 10:01 AM EDT

Opps, forgot to attach extension

executescript.crx
1.4 KB Download

Comment 2 by elawrence@chromium.org on Mon, Apr 24, 2017, 11:34 AM EDT

Cc: fsam...@chromium.org
Components: Platform>Extensions>API

Thanks for the sleuthing!

Comment 3 by mea...@chromium.org on Mon, Apr 24, 2017, 2:01 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: fsam...@chromium.org
Cc: -fsam...@chromium.org
Labels: Security_Severity-Low Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows

Agreed, thanks for the detailed description and the investigation!

According to the severity guidelines, this would normally qualify as a medium severity, but since we consider extension installation a mitigating factor the severity is downgraded to low.

Comment 4 by sheriffbot@chromium.org on Tue, Apr 25, 2017, 9:02 AM EDT

Labels: Pri-2

Comment 5 Deleted

Comment 6 by mbarb...@chromium.org on Wed, Feb 14, 2018, 5:20 PM EST

Owner: rdevl...@chromium.org
Cc: fsam...@chromium.org

Devlin, would you mind taking a look? Reassigning since this seems stale.

Comment 7 by mmoroz@chromium.org on Tue, Apr 30, 2019, 1:52 AM EDT

Labels: M-76

Comment 8 by rdevl...@chromium.org on Mon, Aug 26, 2019, 1:11 PM EDT

Owner: karandeepb@chromium.org
Cc: rdevl...@chromium.org

Revisiting old bugs.

Karan, do you think you can take a look at this? The best solution seems like it would be to surface the extension-relative url (i.e., chrome-extension://<id>/script.js).

Comment 9 by sheriffbot@chromium.org on Wed, Sep 11, 2019, 9:07 AM EDT

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

Comment 10 by sheriffbot@chromium.org on Wed, Oct 23, 2019, 9:17 AM EDT

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

Comment 11 by sheriffbot@chromium.org on Wed, Dec 11, 2019, 9:18 AM EST

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

Comment 12 by rdevl...@chromium.org on Wed, Dec 11, 2019, 6:20 PM EST

Owner: rdevl...@chromium.org

I'll take this one back; I have a patch that should work.

Comment 13 by bugdroid on Fri, Dec 20, 2019, 12:59 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/d52ea54eab4fdedfe640c0838199548c1717b5ed

commit d52ea54eab4fdedfe640c0838199548c1717b5ed
Author: Devlin Cronin <rdevlin.cronin@chromium.org>
Date: Fri Dec 20 17:59:02 2019

[Extensions] Set tabs.executeScript() URLs to chrome-extension: scheme

Set the script URL for scripts executed via chrome.tabs.executeScript()
to use the chrome-extension: scheme, e.g.
chrome-extension://<id>/<path-to-script>, rather than the file URL.
This prevents referencing the filesystem in the URL, and is consistent
with content scripts that are statically specified in the manifest.

Add a regression test (that also tests the statically-defined content
script behavior). This entailed adding a new test utility,
WebContentsConsoleObserver, to track the messages sent to the console
for a given WebContents. This can replace ConsoleObserverDelegate in
the future.

~~Bug: 714617~~
Change-Id: I3de400e6dccf9f9a662824b4810bd52245cd4d62
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/1962676
Reviewed-by: Alex Moshchuk <alexmos@chromium.org>
Reviewed-by: Emily Stark <estark@chromium.org>
Commit-Queue: Devlin <rdevlin.cronin@chromium.org>
Cr-Commit-Position: refs/heads/master@{#726842}

[modify] https://crrev.com/d52ea54eab4fdedfe640c0838199548c1717b5ed/chrome/browser/extensions/content_script_apitest.cc
[modify] https://crrev.com/d52ea54eab4fdedfe640c0838199548c1717b5ed/extensions/browser/api/execute_code_function.cc
[modify] https://crrev.com/d52ea54eab4fdedfe640c0838199548c1717b5ed/extensions/browser/api/execute_code_function.h
[modify] https://crrev.com/d52ea54eab4fdedfe640c0838199548c1717b5ed/extensions/browser/script_executor.cc
[modify] https://crrev.com/d52ea54eab4fdedfe640c0838199548c1717b5ed/extensions/browser/script_executor.h
[modify] https://crrev.com/d52ea54eab4fdedfe640c0838199548c1717b5ed/extensions/common/extension_messages.h
[modify] https://crrev.com/d52ea54eab4fdedfe640c0838199548c1717b5ed/extensions/renderer/programmatic_script_injector.cc

Comment 14 by rdevl...@chromium.org on Fri, Dec 20, 2019, 5:57 PM EST

Status: Fixed (was: Assigned)

This should be fixed with #13.

Given the low impact and duration this has been around, I don't think this is something we need to merge.

Comment 15 by sheriffbot@chromium.org on Sat, Dec 21, 2019, 10:44 AM EST

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

Comment 16 by natashapabrai@google.com on Mon, Jan 6, 2020, 12:57 PM EST

Labels: reward-topanel

Comment 17 by natashapabrai@google.com on Thu, Jan 9, 2020, 11:51 AM 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 18 by natashapabrai@google.com on Thu, Jan 9, 2020, 11:59 AM EST
Congrats! The Panel decided to reward $500 for this report!

Comment 19 by natashapabrai@google.com on Thu, Jan 9, 2020, 12:21 PM EST
Labels: -reward-unpaid reward-inprocess

Comment 20 by adetaylor@google.com on Mon, Mar 9, 2020, 2:19 PM EDT
ngyikp@gmail.com - when this appears in the Chrome release notes, how would you like to be credited?

Comment 21 by ngy...@gmail.com on Mon, Mar 9, 2020, 2:27 PM EDT
You can use my full name: Ng Yik Phang

Comment 22 by adetaylor@google.com on Fri, Mar 13, 2020, 1:44 PM EDT
Labels: Release-0-M81

Comment 23 by adetaylor@chromium.org on Fri, Mar 13, 2020, 2:31 PM EDT
Labels: CVE-2020-6438 CVE_description-missing

Comment 24 by sheriffbot on Sat, Mar 28, 2020, 1:49 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 25 by adetaylor@chromium.org on Tue, Apr 14, 2020, 3:14 PM EDT
Labels: -CVE_description-missing CVE_description-submitted