bugs chromium ▾ New issue Open issues ▾ Search chromium issue ▾ Sign in

☆ Starred by 4 users

Owner:	xiaoc...@chromium.org
CC:	rzanoni@google.com mas...@chromium.org dcheng@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>DataTransfer Blink>SVG Blink>Editing
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-2000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
FoundIn-100
M-101
Target-101
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-4951
merge-merged-101
Release-0-M101
CVE-2022-1492

Issue 1315040: Security: Drag and Drop XSS

Reported by mic...@bentkowski.info on Sun, Apr 10, 2022, 3:35 PM EDT

Code

This bug is similar to many Copy&Paste bugs I reported for Chromium (examples: ~~issue 1011950~~, ~~issue 1040755~~, ~~issue 1065761~~, ~~issue 1141350~~). The difference is that now I'm focusing on drag and drop.

Essentially, when you drag&drop an HTML data into an element that is content-editable, the HTML is automatically sanitized. I used to assume it is the same sanitization process that also works for copy&paste. It turns out that's not the case. I've found a way to execute arbitrary JavaScript on drag&drop by using SVG <use> tag.

Chromium blocks drag&drop for iframes if the target origin is different than the source origin. However, it doesn't block if the drag starts in another window. So the attack scenario is possible, although much less likely than in the case of copy&paste. It is still a bug, though, from a technical stand-point hence I'm reporting it.

Below is a short proof of concept that proves the exploit on the same origin but it also works cross-origin if you drag and drop between two windows (check the attached video; the target is: https://developers-dot-devsite-v2-prod.appspot.com/transliterate/v1/richedittransliteration). Just drag the "drag me" box onto the contenteditable field below to see an alert

```
<!DOCTYPE html>
<meta charset="UTF-8">
<title>Drag And Drop Proof of Concept</title>
<script>const payload = `
  <svg><use href="data:image/svg+xml,&lt;svg id='x' xmlns='http://www.w3.org/2000/svg'&gt;&lt;image href='' onerror='alert(1337)' /&gt;&lt;script&gt;alert(2)&lt;/script&gt;&lt;/svg&gt;#x" />
`;</script>
<div
  style="background:lightblue; padding: 2em; width:100px"
  draggable=true
  ondragstart="event.dataTransfer.setData('text/html', payload)"
>Drag me!</div>
<div contenteditable style="border: 1px solid black; padding:2em; margin-top: 2em; height:200px">Drop here!</div>
```

recording.mov

1.4 MB View Download

[redacted]

Comment 1 by sheriffbot on Sun, Apr 10, 2022, 3:43 PM EDT Project Member

Labels: external_security_report

Comment 2 by rsesek@chromium.org on Mon, Apr 11, 2022, 3:42 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: xiaoc...@chromium.org
Cc: dcheng@chromium.org mas...@chromium.org
Labels: FoundIn-100 Security_Severity-Medium OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-1
Components: Blink>Editing Blink>SVG Blink>DataTransfer

Thanks for the report. I can confirm this on M100 - M102.

Comment 3 by sheriffbot on Mon, Apr 11, 2022, 3:48 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 4 by schenney@chromium.org on Mon, Apr 11, 2022, 7:42 PM EDT Project Member

This is related to another bug where it is argued that we should not execute script in SVG from data urls, which would fix this I believe because we would not run the script in the <use> tag.

Comment 5 by Git Watcher on Mon, Apr 11, 2022, 10:04 PM EDT Project Member

Status: Fixed (was: Assigned)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5164a0fe3391283663e1196cf4576ec233985e89

commit 5164a0fe3391283663e1196cf4576ec233985e89
Author: Xiaocheng Hu <xiaochengh@chromium.org>
Date: Tue Apr 12 02:03:00 2022

Sanitize DragData markup before inserting it into document

~~Fixed: 1315040~~
Change-Id: I8a0ddfb983d12c185f7e943d3d5277788199b011
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3579670
Quick-Run: Xiaocheng Hu <xiaochengh@chromium.org>

Auto-Submit: Xiaocheng Hu <xiaochengh@chromium.org>
Reviewed-by: Kent Tamura <tkent@chromium.org>
Commit-Queue: Kent Tamura <tkent@chromium.org>

Commit-Queue: Kent Tamura <tkent@chromium.org>
Cr-Commit-Position: refs/heads/main@{#991324}

[add]
https://crrev.com/5164a0fe3391283663e1196cf4576ec233985e89/third_party/blink/web_tests/editing/pasteboard/drag-and-drop-svg-use-sanitize.html
[modify]
https://crrev.com/5164a0fe3391283663e1196cf4576ec233985e89/third_party/blink/renderer/core/page/drag_data.cc

Comment 6 by mic...@bentkowski.info on Tue, Apr 12, 2022, 5:18 AM EDT

Wow, that was quick! I checked the fix and it looks fine. Thanks!

Comment 7 by sheriffbot on Tue, Apr 12, 2022, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 8 by sheriffbot on Tue, Apr 12, 2022, 12:51 PM EDT Project Member

Labels: M-101 Target-101

Setting milestone and target because of medium severity.

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

Comment 9 by sheriffbot on Tue, Apr 12, 2022, 1:40 PM EDT Project Member

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

Comment 10 by sheriffbot on Tue, Apr 12, 2022, 2:06 PM EDT Project Member

Labels: Merge-Request-101

Requesting merge to beta M101 because latest trunk commit (991324) appears to be after beta branch point (982481).

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

Comment 11 by sheriffbot on Tue, Apr 12, 2022, 10:04 PM EDT Project Member

Labels: -Merge-Request-101 Merge-Review-101 Hotlist-Merge-Review

Merge review required: M101 is already shipping to beta.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: benmason (Android), harrysouders (iOS), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 12 by xiaoc...@chromium.org on Wed, Apr 13, 2022, 1:31 PM EDT **Project Member**

1. Why does your merge fit within the merge criteria for these milestones?

It's a security fix.

2. What changes specifically would you like to merge? Please link to Gerrit.

https://chromium-review.googlesource.com/c/chromium/src/+/3579670

3. Have the changes been released and tested on canary?

Yes

4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?

No

5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative? https://goto.google.com/cros-engprodcomponents

No, and maybe N/A? This change doesn't have anything specific to ChromeOS

6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Maybe N/A? Because we are not merging to the stable channel

Comment 13 by amyressler@chromium.org on Fri, Apr 15, 2022, 7:46 PM EDT **Project Member**

Labels: -Merge-Review-101 Merge-Approved-101

M101 merge approved, please merge this fix to branch 4951 at your earliest convenience and NLT noon PDT, Tuesday, 19 April

Comment 14 by Git Watcher on Sun, Apr 17, 2022, 9:15 PM EDT **Project Member**

Labels: -merge-approved-101 merge-merged-4951 merge-merged-101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e2b8856012e068e16a9a343525961972bc45b480

commit e2b8856012e068e16a9a343525961972bc45b480
Author: Xiaocheng Hu <xiaochengh@chromium.org>
Date: Mon Apr 18 01:14:45 2022

[M101] Sanitize DragData markup before inserting it into document

(cherry picked from commit 5164a0fe3391283663e1196cf4576ec233985e89)

~~Fixed: 1315040~~

Change-Id: I8a0ddfb983d12c185f7e943d3d5277788199b011
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3579670
Quick-Run: Xiaocheng Hu <xiaochengh@chromium.org>

Quick-Run: Xiaocheng Hu <xiaochengh@chromium.org>
Auto-Submit: Xiaocheng Hu <xiaochengh@chromium.org>
Reviewed-by: Kent Tamura <tkent@chromium.org>
Commit-Queue: Kent Tamura <tkent@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#991324}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3588887
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4951@{#831}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[add] https://crrev.com/e2b8856012e068e16a9a343525961972bc45b480/third_party/blink/web_tests/editing/pasteboard/drag-and-drop-svg-use-sanitize.html
[modify] https://crrev.com/e2b8856012e068e16a9a343525961972bc45b480/third_party/blink/renderer/core/page/drag_data.cc

Comment 15 by sheriffbot on Sun, Apr 17, 2022, 9:22 PM EDT Project Member

Labels: LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 16 by rzanoni@google.com on Mon, Apr 18, 2022, 9:44 AM EDT Project Member

Cc: rzanoni@google.com
Labels: LTS-Evaluating-96

Comment 17 by rzanoni@google.com on Mon, Apr 18, 2022, 1:24 PM EDT Project Member

Labels: -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 18 by sheriffbot on Mon, Apr 18, 2022, 1:28 PM EDT Project Member

Labels: -LTS-Merge-Request-96 LTS-Merge-Review-96

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 19 by rzanoni@google.com on Mon, Apr 18, 2022, 1:38 PM EDT Project Member

1. Just https://crrev.com/c/3589799
2. Low, no conflicts
3. 101
4. Yes

Comment 20 by gmpritchard@google.com on Tue, Apr 19, 2022, 10:27 AM EDT Project Member

Labels: -LTS-Merge-Candidate LTS-Merge-Delayed-96

Comment 21 by amyressler@google.com on Thu, Apr 21, 2022, 8:40 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-2000

*** 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 22 by amyressler@chromium.org on Thu, Apr 21, 2022, 9:57 PM EDT Project Member

Thank you for this report! The VRP Panel has decided to award you $2,000 for your report of this issue. Thank you for your efforts and taking the time to report this to us.

Comment 23 by mic...@bentkowski.info on Fri, Apr 22, 2022, 7:36 AM EDT

Thanks!

Comment 24 by gmpritchard@google.com on Fri, Apr 22, 2022, 12:41 PM EDT Project Member

Labels: -LTS-Merge-Review-96 -LTS-Merge-Delayed-96 LTS-Merge-Approved-96

Comment 25 by amyressler@chromium.org on Mon, Apr 25, 2022, 12:44 PM EDT Project Member

Labels: Release-0-M101

Comment 26 by amyressler@google.com on Mon, Apr 25, 2022, 4:07 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 27 by Git Watcher on Mon, Apr 25, 2022, 4:58 PM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/12ba78f3fa7a42c9a6a15f7a8248453ffef91a08

commit 12ba78f3fa7a42c9a6a15f7a8248453ffef91a08
Author: Xiaocheng Hu <xiaochengh@chromium.org>

Author: Xiaocheng Hu <xiaochengh@chromium.org>
Date: Mon Apr 25 20:57:43 2022

[M96-LTS] Sanitize DragData markup before inserting it into document

(cherry picked from commit 5164a0fe3391283663e1196cf4576ec233985e89)

~~Fixed: 1315040~~
Change-Id: I8a0ddfb983d12c185f7e943d3d5277788199b011
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3579670
Quick-Run: Xiaocheng Hu <xiaochengh@chromium.org>
Auto-Submit: Xiaocheng Hu <xiaochengh@chromium.org>
Commit-Queue: Kent Tamura <tkent@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#991324}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3589799
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Owners-Override: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1602}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[add] https://crrev.com/12ba78f3fa7a42c9a6a15f7a8248453ffef91a08/third_party/blink/web_tests/editing/pasteboard/drag-and-drop-svg-use-sanitize.html
[modify] https://crrev.com/12ba78f3fa7a42c9a6a15f7a8248453ffef91a08/third_party/blink/renderer/core/page/drag_data.cc

Comment 28 by rzanoni@google.com on Tue, Apr 26, 2022, 9:38 AM EDT Project Member

Labels: -LTS-Merge-Approved-96 LTS-Merge-Merged-96

Comment 29 by amyressler@google.com on Tue, Apr 26, 2022, 4:32 PM EDT Project Member

Labels: CVE-2022-1492 CVE_description-missing

Comment 30 by sheriffbot on Wed, Jul 20, 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 31 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 32 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing