☆ Starred by 4 users

Owner:	vogelheim@chromium.org
CC:	koto@google.com ecenazo@google.com aaronshim@google.com amyressler@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>SecurityFeature>TrustedTypes
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
M-100
Reward-1000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
FoundIn-83
external_security_report
Target-100
Release-0-M101
CVE-2022-1494

Issue 1298122: Security: TrustedTypes does not block assignment when modifying existing attribute value via nodeValue/textContent

Reported by masat...@gmail.com on Wed, Feb 16, 2022, 1:40 PM EST

Code

VULNERABILITY DETAILS

TrustedTypes blocks the following cases:

```
iframe.setAttribute('srcdoc','XSS');//blocked
iframe.srcdoc='XSS';//blocked
```

But if the existing attribute value is modified via the nodeValue or textContent property, it does not block the assignment. e.g.:

```
iframe.attributes.srcdoc.nodeValue='XSS';
iframe.attributes.srcdoc.textContent='XSS';
```

This should be expected to be blocked.

VERSION

Version 100.0.4892.0 (Official Build) canary (64-bit)

REPRODUCTION CASE

You can reproduce it here: https://vulnerabledoma.in/ttbypass_attr_nodeValue_textContent.html

I attached the same HTML.

CREDIT INFORMATION

Reporter credit: Masato Kinugawa

ttbypass_attr_nodeValue_textContent.html

492 bytes View Download

Comment 1 by sheriffbot on Wed, Feb 16, 2022, 1:43 PM EST Project Member

Labels: external_security_report

Comment 2 by yelizaveta@google.com on Wed, Feb 16, 2022, 2:12 PM EST Project Member

Status: WontFix (was: Unconfirmed)

frame-src needs to be set in the CSP in order to lock the iframe src attribute. This also is not a chrome specific vulnerability.

If you get a working exploit with frame-src enabled in the CSP I recommend filing the bug at https://bughunters.google.com/report.

Comment 3 by masat...@gmail.com on Wed, Feb 16, 2022, 2:23 PM EST

This is not a CSP bypass but it is a TrustedTypes bypass. TruesedTypes is a security feature to block the "assignment" itself (not the script execution).

Comment 4 by masat...@gmail.com on Wed, Feb 16, 2022, 3:16 PM EST

Note that these assignments are not blocked not only for the srcdoc attribute but also for other XSS sinks, which should be blocked (e.g. event handler, script-src).
I created the PoC for the script-src and onclick: https://vulnerabledoma.in/ttbypass_attr_nodeValue_textContent2.html

ttbypass_attr_nodeValue_textContent2.html
517 bytes View Download

Comment 5 by koto@google.com on Tue, Feb 22, 2022, 12:32 PM EST Project Member

Components: Blink>SecurityFeature>TrustedTypes

Comment 6 by koto@google.com on Tue, Feb 22, 2022, 12:34 PM EST Project Member

Status: Available (was: WontFix)

Comment 7 by koto@google.com on Wed, Feb 23, 2022, 7:59 AM EST Project Member

Owner: vogelheim@google.com

Daniel, can you look at these? I think this is mentioning the attribute node direct modification, the most relevant bits being described https://github.com/w3c/webappsec-trusted-types/issues/248#issuecomment-576373688.

Comment 8 by koto@google.com on Wed, Feb 23, 2022, 8:08 AM EST Project Member

Cc: koto@google.com

Comment 9 by danakj@chromium.org on Wed, Feb 23, 2022, 12:06 PM EST Project Member

Status: Assigned (was: Available)
Labels: Security_Severity-Medium OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-2

I've attempted to open the repro but I am not sure what it demonstrates. I just see 2 imgs that are not loaded, so it's hard to check what versions of Chrome it would repro in.

Comment 10 by sheriffbot on Thu, Feb 24, 2022, 1:18 PM EST Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. 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 11 by vogelheim@chromium.org on Thu, Mar 3, 2022, 8:51 AM EST Project Member

Status: Started (was: Assigned)

Can repro. I agree this is a Trusted Types bypass, and particularly agree with #c0, #c3 and #c4.

(No idea what to do with this, yet.)

Comment 12 by vogelheim@chromium.org on Thu, Mar 3, 2022, 8:51 AM EST Project Member

Owner: vogelheim@chromium.org

Comment 13 by vogelheim@chromium.org on Thu, Mar 3, 2022, 9:20 AM EST Project Member

[still tentative]

Most DOM Node apis have an external (JS-callable) version and an internal one, where the JS-callable one does additional checks, while the internal one is expected to do as it's told. A common pattern is that the JS-callable one has an ExceptionState argument, and the internal one doesn't. For Attr::setAttribute this applies as well. It turns out that:

- Attr::setNodeValue doesn't take an ExceptionState
- it calls the ExceptionState-less Attr::setAttribute
- ExceptionState-less Attr::setAttribute doesn't run the TT check, because 1, it looks like it'd be internal-use only, and 2, it doesn't have an ExceptionState to report the exception to.

The net result is that setting the nodeValue on a DOM Attribute node doesn't ever run the TT check, while setting the attribute directly would have.

Comment 14 by vogelheim@chromium.org on Tue, Mar 8, 2022, 7:21 AM EST Project Member

Fix in progress, crrev.com/c/3497765.

Comment 15 by Git Watcher on Mon, Mar 14, 2022, 9:05 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/9903cb3f093dd569bbc19aaab525cd0239a98366

commit 9903cb3f093dd569bbc19aaab525cd0239a98366
Author: Daniel Vogelheim <vogelheim@chromium.org>
Date: Mon Mar 14 13:04:04 2022

[Trusted Types] Ensure Trusted Types check runs on all Attr methods.

Ensure that assigning to a DOM attribute's nodeValue or
textContent property runs the same checks as calling setValue.

~~BUG: 1298122~~
Change-Id: Ia71f18ca98a4bcea58ec1014c71bcb0944d9aecb
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3503905
Reviewed-by: Yifan Luo <lyf@chromium.org>
Reviewed-by: Mason Freed <masonf@chromium.org>
Commit-Queue: Daniel Vogelheim <vogelheim@chromium.org>
Cr-Commit-Position: refs/heads/main@{#980525}

[modify] https://crrev.com/9903cb3f093dd569bbc19aaab525cd0239a98366/third_party/blink/renderer/core/dom/character_data.cc
[modify] https://crrev.com/9903cb3f093dd569bbc19aaab525cd0239a98366/third_party/blink/renderer/core/dom/character_data.h
[modify] https://crrev.com/9903cb3f093dd569bbc19aaab525cd0239a98366/third_party/blink/renderer/core/dom/node.idl
[modify] https://crrev.com/9903cb3f093dd569bbc19aaab525cd0239a98366/third_party/blink/renderer/core/dom/node.h
[modify] https://crrev.com/9903cb3f093dd569bbc19aaab525cd0239a98366/third_party/blink/renderer/core/dom/attr.h
[modify] https://crrev.com/9903cb3f093dd569bbc19aaab525cd0239a98366/third_party/blink/renderer/core/dom/node.cc
[add] https://crrev.com/9903cb3f093dd569bbc19aaab525cd0239a98366/third_party/blink/web_tests/external/wpt/trusted-types/block-string-assignment-to-attribute-via-attribute-node.tentative.html
[modify] https://crrev.com/9903cb3f093dd569bbc19aaab525cd0239a98366/third_party/blink/renderer/core/dom/attr.cc

Comment 16 by vogelheim@chromium.org on Mon, Mar 14, 2022, 1:53 PM EDT Project Member

Status: Fixed (was: Started)
Labels: FoundIn-83

Should be fixed now. Thanks for the report!

(Explanation in #c13 was correct. Link in #c14 was incorrect; #c15 is the correct CL.)

I set FoundIn to M83, which is when TT was launched, since I think this bug has been in since the initial release.

Comment 17 by sheriffbot on Mon, Mar 14, 2022, 1:58 PM EDT Project Member

Status: Assigned (was: Fixed)

Dear owner, thanks for fixing this bug. We've reopened it because security bugs need Security_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches (as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact (security@chromium.org) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines: https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues FoundIn guidelines: https://chromium.googlesource.com/chromium/src/+/main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security Thanks for your time!

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

Comment 18 by sheriffbot on Mon, Mar 14, 2022, 1:58 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 19 by vogelheim@chromium.org on Wed, Mar 16, 2022, 7:14 AM EDT Project Member

Labels: -Security_Impact-Extended Security_Impact-Stable

Comment 20 by vogelheim@chromium.org on Wed, Mar 16, 2022, 7:15 AM EDT Project Member

Status: Fixed (was: Assigned)

Comment 21 by sheriffbot on Wed, Mar 16, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 22 by sheriffbot on Wed, Mar 16, 2022, 12:52 PM EDT Project Member

Labels: M-100 Target-100

Setting milestone and target because of medium severity.

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

Comment 23 by sheriffbot on Wed, Mar 16, 2022, 1:42 PM EDT Project Member

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

Comment 24 by sheriffbot on Wed, Mar 16, 2022, 2:13 PM EDT Project Member

Labels: Merge-Request-100

Requesting merge to beta M100 because latest trunk commit (980525) appears to be after beta branch point (972766).

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

Comment 25 by sheriffbot on Wed, Mar 16, 2022, 2:19 PM EDT Project Member

Labels: -Merge-Request-100 Hotlist-Merge-Review Merge-Review-100

Merge review required: M100 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: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 26 by gov...@chromium.org on Wed, Mar 16, 2022, 3:46 PM EDT Project Member

Cc: amyressler@chromium.org

Comment 27 by amyressler@chromium.org on Thu, Mar 17, 2022, 1:59 PM EDT Project Member

Labels: -Merge-Review-100 Merge-Approved-100

M100 merge approved; please merge this fix to branch 4896 NLT 12p PDT/8p CET Monday, 21 March so this fix can be included in M100 stable cut -- thank you

Comment 28 by amyressler@chromium.org on Fri, Mar 18, 2022, 12:15 PM EDT Project Member

Labels: -Merge-Approved-100

after talking off-bug to a vogelheim@, there is moderate risk with introducing this fix to M100 stable; removing merge approval and letting this fix matriculate into M101 rather than be merged to stable at this time

Comment 29 by vogelheim@chromium.org on Fri, Mar 18, 2022, 12:19 PM EDT Project Member

#c25:
1.This is a security fix. The release guidelines do say, "any security issue", so it should be in scope.
2. #c15 (https://chromium-review.googlesource.com/c/chromium/src/+/3503905)
3. Yes, but not for long. This landed only this week.
4. No.
5. n/a
6. n/a

Generally, I'm a bit skeptical on a backmerge just before stable:
- IMHO, the fix is medium risky, on grounds that the code area (DOM implementation) is fairly fundamental, but I don't know

- IMHO, the fix is medium risky, on grounds that the code area (DOM implementation) is fairly fundamental, but I don't know it super well.
- IMHO, the risk of the underlying security issue is moderate, since it isn't exploitable by itself and has been in the code for a while.

Overall, I'd be happier if the fix had a bit more time to "bake in". Of course, I'll be happy to follow whatever decision the release folks take.

Comment 30 by vogelheim@google.com on Wed, Mar 23, 2022, 10:05 AM EDT Project Member

Cc: aaronshim@google.com

Comment 31 by amyressler@google.com on Thu, Mar 31, 2022, 5:15 PM EDT 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.

Please contact security-vrp@chromium.org with any questions.
****

Comment 32 by amyressler@chromium.org on Thu, Mar 31, 2022, 5:38 PM EDT Project Member

Congratulations, Masato! The VRP Panel would like to extend to you a $1,000 reward for this issue. Thank you for your efforts and reporting this issue to us!

Comment 33 by amyressler@google.com on Fri, Apr 1, 2022, 4:11 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 34 by vogelheim@chromium.org on Tue, Apr 5, 2022, 11:04 AM EDT Project Member

Cc: ecenazo@google.com

Comment 35 by amyressler@chromium.org on Mon, Apr 25, 2022, 8:40 PM EDT Project Member

Labels: Release-0-M101

Comment 36 by amyressler@google.com on Tue, Apr 26, 2022, 4:32 PM EDT Project Member

Labels: CVE-2022-1494 CVE_description-missing

Comment 37 by sheriffbot on Wed, Jun 22, 2022, 1:31 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

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

Comment 38 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 39 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing