Starred by 3 users

Owner:	rdevl...@chromium.org
CC:	rzanoni@google.com amyressler@chromium.org
Status:	Fixed *(Closed)*
Components:	Platform>Extensions
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
M-100
Reward-1000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
Target-100
FoundIn-99
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-4896
merge-merged-100
Release-0-M100
CVE-2022-1145

Issue 1304545: Security: Potential Use After Free in ManagedValueStoreCache::OnPolicyUpdated

Reported by vigi...@gmail.com on Wed, Mar 9, 2022, 2:19 AM EST

Code

A potential UAF in |ManagedValueStoreCache::OnPolicyUpdated| by auditing. This method posts a backend task. The posted OnceCallback is |ManagedValueStoreCache::UpdatePolicyOnBackend| with raw pointer |this|.[1] This may potential trigger an UAF issue when the backend thread run the callback after delete ManagedValueStoreCache instance.

[1] https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/extensions/api/storage/managed_value_store_cache.cc;l=323

In |SyncValueStoreCache::SyncValueStoreCache| there is also a similar code snippets but it's in constructor so it's safe. However |ManagedValueStoreCache::OnPolicyUpdated| is not in this circumstances.

I have no idea how to reproduce this. I didn't figure out how to trigger |ManagedValueStoreCache::OnPolicyUpdated| by my hand. Maybe update extension with new policy? Or write some browser test code?

Comment 1 by sheriffbot on Wed, Mar 9, 2022, 2:24 AM EST Project Member

Labels: external_security_report

Comment 2 by bookholt@chromium.org on Wed, Mar 9, 2022, 7:13 PM EST Project Member

Components: Platform>Extensions

Thanks for the report!

If I understand correctly, this seems to be a general concern about raw pointer usage. Have you found a specific way to trigger a UAF, such as how the callback might run after deleting the associated ManagedValueStoreCache instance? We'll need some more details about specific ways things break in order to treat this report as a security issue.

Leaving this open for now, and will revisit later in the week to close as WontFix (Working as intended) if no additional details are available.

Comment 3 by vigi...@gmail.com on Fri, Mar 11, 2022, 1:45 AM EST

|GetBackendTaskRunner| here is the same as |GetExtensionFileTaskRunner| which is a |LazyThreadPoolSequencedTaskRunner|. The callback task in it should consider thread switch. The UAF potentially occurs when thread switch after deleting SyncValueStoreCache instance.

This is why use |GetBackendTaskRunner| should consider using weakptr. Some examples are: https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/extensions/api/storage/managed_value_store_cache.cc;l=173

Unless the class or method is designed to be safe like: https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/extensions/api/storage/sync_value_store_cache.cc;l=48 https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/extensions/pack_extension_job.cc;l=40

Comment 4 by bookholt@chromium.org on Mon, Mar 14, 2022, 12:51 PM EDT Project Member

Owner: rdevl...@chromium.org
Labels: FoundIn-99 OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows

Redirecting to the subsystem owner for assistance with prioritization and severity assessment.

Comment 5 by sheriffbot on Mon, Mar 14, 2022, 12:57 PM EDT Project Member

Labels: Security_Impact-Stable

Comment 6 by rdevl...@chromium.org on Mon, Mar 14, 2022, 8:30 PM EDT Project Member

Status: Started (was: Unconfirmed)

Interesting; good find!

In practice, I'm not sure how exploitable this is - you'd have to trigger a policy update right before a profile is deleted, and I'm not sure if there's any good way (short of native execution) to trigger that sequence of events. However, I definitely agree that it is theoretically possible, and definitely unsafe usage and a bug. I'll get a CL up to fix this.

Comment 7 by Git Watcher on Tue, Mar 15, 2022, 8:12 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b501c4e45aeb23261b57e6f44ece15f8b4c977fa

commit b501c4e45aeb23261b57e6f44ece15f8b4c977fa
Author: Devlin Cronin <rdevlin.cronin@chromium.org>
Date: Wed Mar 16 00:11:10 2022

[Extensions] Use a WeakPtr in ManagedValueStoreCache

When posting a task, use a WeakPtr instead of base::Unretained().

~~Bug: 1304545~~
Change-Id: I5b2a1e48366a9d0dfaae9f4414f4336cdd5b4a2f
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3523211
Reviewed-by: David Bertoni <dbertoni@chromium.org>
Commit-Queue: Devlin Cronin <rdevlin.cronin@chromium.org>
Cr-Commit-Position: refs/heads/main@{#981406}

[modify]
https://crrev.com/b501c4e45aeb23261b57e6f44ece15f8b4c977fa/chrome/browser/extensions/api/storage/managed_value_store_cache.h
[modify]
https://crrev.com/b501c4e45aeb23261b57e6f44ece15f8b4c977fa/chrome/browser/extensions/api/storage/managed_value_store_cache.cc

Comment 8 by rdevl...@chromium.org on Tue, Mar 15, 2022, 9:01 PM EDT Project Member

Status: Fixed (was: Started)

This should be fixed with the CL above.

I'll leave it to the security team whether this deserves a merge (see also c#6).

Comment 9 by sheriffbot on Tue, Mar 15, 2022, 9:03 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 10 by bookholt@chromium.org on Tue, Mar 15, 2022, 9:05 PM EDT Project Member

Labels: Security_Severity-Medium Pri-2

Thanks for the fix!

Based on comment 6, this bug meets the criteria for medium severity by my interpretation of the severity guidelines: https://chromium.googlesource.com/chromium/src/+/HEAD/docs/security/severity-guidelines.md#toc-medium-severity

Comment 11 by bookholt@chromium.org on Tue, Mar 15, 2022, 9:06 PM EDT Project Member

Status: Fixed (was: Assigned)

Ah, sheriffbot beat me to it. Re-closing.

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

Labels: reward-topanel

Comment 13 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 14 by sheriffbot on Wed, Mar 16, 2022, 1:18 PM EDT 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 15 by sheriffbot on Wed, Mar 16, 2022, 1:42 PM EDT Project Member

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

Comment 16 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 (981406) appears to be after beta branch point (972766).

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

Comment 17 by sheriffbot on Wed, Mar 16, 2022, 8:14 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 18 by amyressler@chromium.org on Thu, Mar 17, 2022, 2:09 PM EDT Project Member

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

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

Comment 19 by sheriffbot on Mon, Mar 21, 2022, 12:22 PM EDT Project Member

Cc: amyressler@chromium.org

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 20 by srinivassista@google.com on Mon, Mar 21, 2022, 6:18 PM EDT Project Member

CP here - https://chromium-review.googlesource.com/c/chromium/src/+/3540974 for M100, please help land it.

Comment 21 by Git Watcher on Mon, Mar 21, 2022, 7:34 PM EDT Project Member

Labels: -merge-approved-100 merge-merged-4896 merge-merged-100

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/abdc96c71a384d94fda6c6687b19685d20292b61

commit abdc96c71a384d94fda6c6687b19685d20292b61
Author: Daylin Cronin <daylin.cronin@chromium.org>

Author: Devlin Cronin <rdevlin.cronin@chromium.org>
Date: Mon Mar 21 23:33:14 2022

[Extensions] Use a WeakPtr in ManagedValueStoreCache

When posting a task, use a WeakPtr instead of base::Unretained().

(cherry picked from commit b501c4e45aeb23261b57e6f44ece15f8b4c977fa)

~~Bug: 1304545~~
Change-Id: I5b2a1e48366a9d0dfaae9f4414f4336cdd5b4a2f
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3523211
Reviewed-by: David Bertoni <dbertoni@chromium.org>
Commit-Queue: Devlin Cronin <rdevlin.cronin@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#981406}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3540974
Reviewed-by: Krishna Govind <govind@chromium.org>
Owners-Override: Krishna Govind <govind@chromium.org>
Commit-Queue: Srinivas Sista <srinivassista@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#763}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/abdc96c71a384d94fda6c6687b19685d20292b61/chrome/browser/extensions/api/storage/managed_value_store_cache.h
[modify]
https://crrev.com/abdc96c71a384d94fda6c6687b19685d20292b61/chrome/browser/extensions/api/storage/managed_value_store_cache.cc

Comment 22 by sheriffbot on Mon, Mar 21, 2022, 7:35 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 23 by rzanoni@google.com on Tue, Mar 22, 2022, 5:39 AM EDT Project Member

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

Comment 24 by rzanoni@google.com on Tue, Mar 22, 2022, 7:50 AM EDT Project Member

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

Comment 25 by sheriffbot on Tue, Mar 22, 2022, 7:54 AM 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 26 by rzanoni@google.com on Tue, Mar 22, 2022, 8:09 AM EDT Project Member

1. Just https://crrev.com/c/3541979
2. Low, just include conflicts
3. 100
4. Yes

Comment 27 by gmpritchard@google.com on Tue, Mar 22, 2022, 12:15 PM EDT Project Member

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

Comment 28 by amyressler@chromium.org on Mon, Mar 28, 2022, 5:33 PM EDT Project Member

Labels: Release-0-M100

Comment 29 by vigi...@gmail.com on Mon, Mar 28, 2022, 10:09 PM EDT

Please credit to Yakun Zhang of Baidu Security.

Comment 30 by amyressler@google.com on Tue, Mar 29, 2022, 1:15 PM EDT Project Member

Labels: CVE-2022-1145 CVE_description-missing

Comment 31 by gmpritchard@google.com on Tue, Mar 29, 2022, 1:32 PM EDT Project Member

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

Comment 32 by gmpritchard@google.com on Tue, Mar 29, 2022, 4:50 PM EDT Project Member

Labels: -LTS-Merge-Delayed-96

Comment 33 by Git Watcher on Thu, Mar 31, 2022, 1:09 PM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b9b2d92171974f464277f53e82222cc58ab406c6

commit b9b2d92171974f464277f53e82222cc58ab406c6
Author: Devlin Cronin <rdevlin.cronin@chromium.org>
Date: Thu Mar 31 17:08:31 2022

[M96-LTS][Extensions] Use a WeakPtr in ManagedValueStoreCache

M96 merge issues:
  Conflicting includes

When posting a task, use a WeakPtr instead of base::Unretained().

(cherry picked from commit b501c4e45aeb23261b57e6f44ece15f8b4c977fa)

~~Bug: 1304545~~
Change-Id: I5b2a1e48366a9d0dfaae9f4414f4336cdd5b4a2f
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3523211
Commit-Queue: Devlin Cronin <rdevlin.cronin@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#981406}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3541979
Reviewed-by: Michael Ershov <miersh@google.com>
Owners-Override: Michael Ershov <miersh@google.com>
Commit-Queue: Michael Ershov <miersh@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1563}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/b9b2d92171974f464277f53e82222cc58ab406c6/chrome/browser/extensions/api/storage/managed_value_store_cache.h
[modify]
https://crrev.com/b9b2d92171974f464277f53e82222cc58ab406c6/chrome/browser/extensions/api/storage/managed_value_store_cache.cc

Comment 34 by voit@google.com on Fri, Apr 1, 2022, 8:22 AM EDT Project Member

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

Comment 35 by amyressler@google.com on Fri, Apr 15, 2022, 1:09 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 36 by amyressler@chromium.org on Fri, Apr 15, 2022, 1:21 PM EDT Project Member

Hello, Yakun Zhang and thank you for your report! As this report was lacking a poc or information on how this issue could be exploited, it would not ordinarily be eligible for a VRP reward, but we are extending to you a thank you reward as we did land a fix that would mitigate against any potential security consequences. Thank you for your efforts and reporting this issue to us!

Comment 37 by amyressler@google.com on Fri, Apr 15, 2022, 9:56 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 38 by vigi...@gmail.com on Mon, Apr 18, 2022, 3:34 AM EDT

Hello amyressler, thank you for the rewards. I'm definitely understand the VRP reward rules. Thank you. However, I think this issue's condition is very similar with ~~issue 1248438~~. Which is also no PoC and a medium severity potential browser process UAF. And it rewards 10000. Can you please explain some reasons and I will take the experience for the future research. Thank you.

Comment 39 by amyressler@chromium.org on Mon, Apr 18, 2022, 2:03 PM EDT Project Member

Hello, there was not evidence in the report nor on the analysis on our side - by the security sheriff or the developer/extensions SME- that this issue has security implications or is exploitable. As per comment #6, analysis lends to the contrary - as it appears this issue is likely not exploitable and even if potentially so, the potential is low and is heavily mitigated by needing to trigger a policy update right before profile deletion.
As always, if you can demonstrate exploitability and performing with - or especially without - these mitigations we would happily revisit and reassess for a potential increase in the reward amount. Thanks!

Comment 40 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

Comment 41 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 42 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing