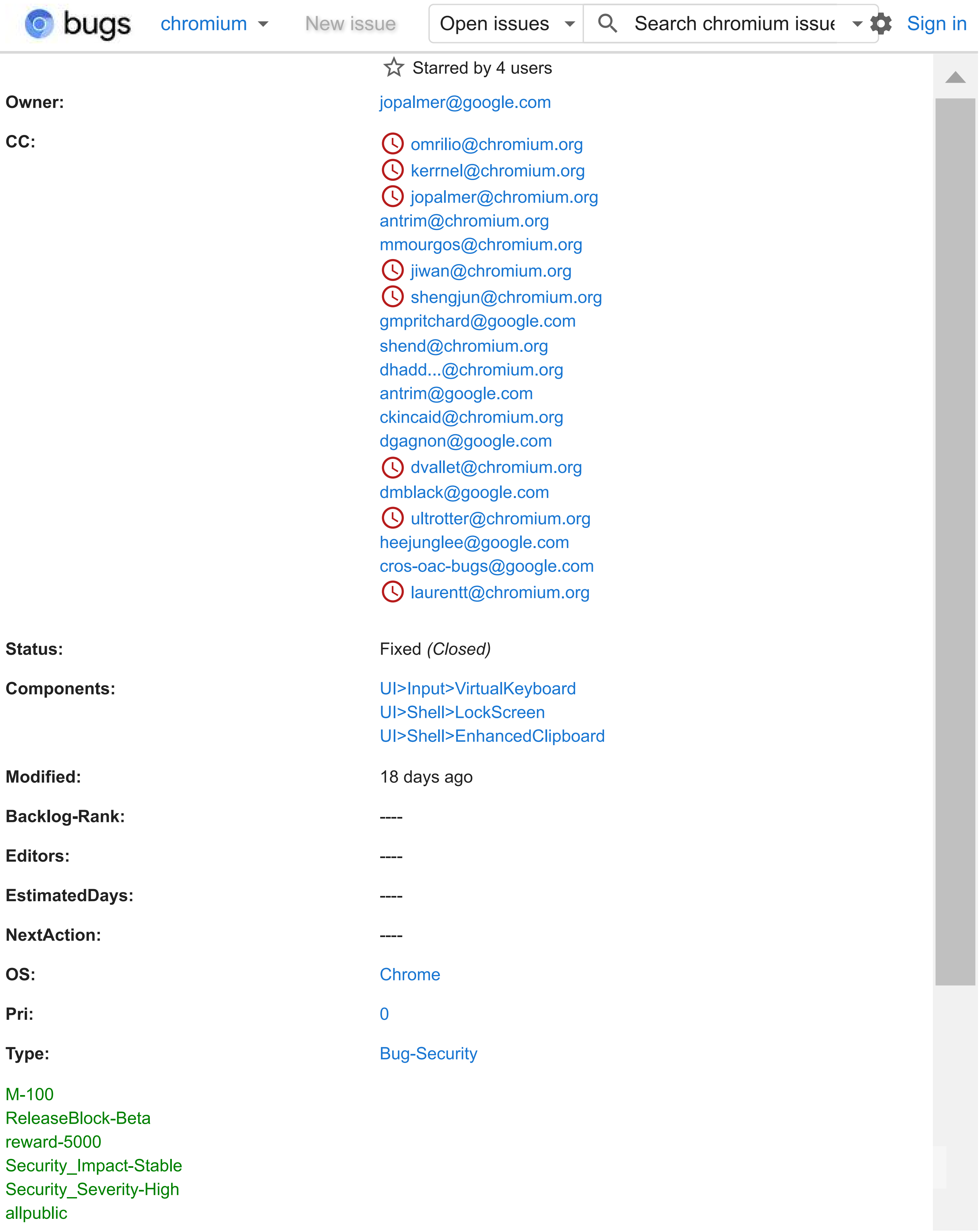

☆ Starred by 4 users

Owner:	jopalmer@google.com
CC:	omrilio@chromium.org kerrnel@chromium.org jopalmer@chromium.org antrim@chromium.org mmourgos@chromium.org jiwan@chromium.org shengjun@chromium.org gmpritchard@google.com shend@chromium.org dhadd...@chromium.org antrim@google.com ckincaid@chromium.org dgagnon@google.com dvallet@chromium.org dmblack@google.com ultrotter@chromium.org heejunglee@google.com cros-oac-bugs@google.com laurentt@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Input>VirtualKeyboard UI>Shell>LockScreen UI>Shell>EnhancedClipboard
Modified:	18 days ago
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Chrome
Pri:	0
Type:	Bug-Security

M-100
ReleaseBlock-Beta
reward-5000
Security_Impact-Stable
Security_Severity-High
allpublic

reward-inprocess
CVE_description-submitted
Restrict-AddIssueComment-scr2b-migration

Issue 1303410: Security: ChromeOS - Lockscreen leaks clipboard contents, i.a.

Reported by hesse...@googlemail.com on Sun, Mar 6, 2022, 3:57 PM EST

Code

Only users with scr2b-migration permission or issue reporter may comment.

⚠ This issue has moved to b/258075040. Updates should be posted in b/258075040.

Hello,

Today I used my Chromebook

* v99.0.4844.57

with the on-screen keyboard on the touchscreen. So far, so good.

Unfortunately, my sleepy eyes had to notice that the clipboard contents are leaked on the lockscreen. I am wondering, why.

How?
========

Simply find a textbox, here the several textboxes for adding a VPN:

0.) Be in front of the device, the user has locked his session (not: logged out)
1.) press the menu (clock) in the lower right corner
==> some quick tiles are appearing
2.) Search the "VPN" icon and press its subtext
==> you get a dark menu "Privates Netzwerk" (Private Network), showing two entries with a plus sign at their rights
3.) click the plus sign next to the first entry
==> You get the mask "Mit VPN verbinden" for setting up a VPN
4.) Select a textbox

Voilà: The on-screen keyboard is suggesting to insert the clipboard contents into the textbox. A tiny preview is shown within the top multifunctional bar. Simply press the preview and enjoy reading the whole clipboard text.

Problem:
========
The clipboard may contain high sensitive and/or personal data of every kind (financial, sexual, religiuos, PINs, password, bitcoin etc.). These do not have to be exposed to local proximate attackers.

Even if the VPN option would be removed in regard of an other ticket, the behaviour would be still abusable, as nobody can guarantee that the system is not offering other textboxes somewhere, currently and/or in the future.

Expectation:
=============
The "suggestion bar" must not provide the clipboard contents (which were stored within an unlocked session) on the lockscreen, quasi accessible to everyone.

Side notes:
============

Possibily two additional vulnerabilities in this connection:

1.) Once pasted via on-screen keyboard, Ctrl-V on the hardware keyboard is also suddenly working (although Ctrl-V is generally disabled!?!)

2.) The "word-suggestions bar" was suggesting my private words on the lockscreen. These words were manually stored within the keyboard settings.

I assume that you do not need separate tickets for these.

Thank you for checking and fixing, for my and millions of others security.

Best regards

Show 2 older comments

Comment 3 by dcheng@chromium.org on Mon, Mar 7, 2022, 2:50 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Labels: OS-Chrome

Reproduced. Over to the CrOS security queue.

Comment 4 by dcheng@chromium.org on Mon, Mar 7, 2022, 8:00 PM EST Project Member

Status: Unconfirmed (was: Assigned)

Comment 5 by kerrnel@google.com on Tue, Mar 8, 2022, 4:37 PM EST Project Member

Status: Available (was: Unconfirmed)
Labels: Security_Severity-Critical FoundIn-99 Pri-0
Components: UI>Shell>LockScreen

Thanks for this report. Lock screen bypasses are a P-0 in our publicly documented severity guidelines: https://chromium.googlesource.com/chromiumos/docs/+/HEAD/security_severity_guidelines.md#critical-severity

Comment 6 by sheriffbot on Tue, Mar 8, 2022, 4:40 PM EST Project Member

Labels: Security_Impact-Stable

Comment 7 by kerrnel@google.com on Tue, Mar 8, 2022, 5:57 PM EST Project Member

Labels: Pri-1

Downgrading to P-1 as this is an information leak, not a lockscreen bypass, after discussion with the team.

Comment 8 by hesse...@googlemail.com on Wed, Mar 9, 2022, 1:00 AM EST

Thank you for the information that repairing will take place the next weeks.

Regarding "lockscreen bypass": In context with this ticket I want to awake the related ~~Issue 1300710~~ and 1303312 into memories (unfortunately, the ticket's title has a copy-paste error, don't get fooled).

Issue: Copy clipboard on locked devices and paste it in the unlocked session. Probably a lock screen bypass as manipulation is possible.
Especially issue 1303312, as it is video documenting the vulnerability.

Comment 9 by kerrnel@google.com on Wed, Mar 9, 2022, 12:42 PM EST Project Member

Status: Assigned (was: Available)
Owner: ultrotter@chromium.org

Comment 10 by kerrnel@google.com on Wed, Mar 9, 2022, 12:43 PM EST Project Member

Cc: antrim@chromium.org

Comment 11 by kerrnel@google.com on Wed, Mar 9, 2022, 12:44 PM EST Project Member

Cc: antrim@google.com

Comment 12 by sheriffbot on Wed, Mar 9, 2022, 12:47 PM EST Project Member

Labels: M-99 Target-99

Setting milestone and target because of high severity.

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

Comment 13 by antrim@chromium.org on Wed, Mar 9, 2022, 12:55 PM EST Project Member

Owner: oka@chromium.org

Interesting, this seems to be a Virtual Keybard problem: ChromeOS has separate clipboards for in-session and lock screen (there is even a browser test to check that: https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ash/login/session/chrome_session_manager_browsertest.cc;drc=6c453d783a46e0c36bf578025d13bb28df1ffffa;l=188), but VK seems to ignore this restriction.
Assigning to an engineer from Virtual Keyboard team.

Comment 14 by antrim@chromium.org on Wed, Mar 9, 2022, 1:01 PM EST Project Member

Verified on Chrome 1010.4940: direct paste (via Ctrl-V) does not expose data from session, triggering vk via accessibility menu does not expose clipboard, but turning device into tablet mode and focusing on some input field (e.g. VPN network name in this case) does expose clipboard contents.

Comment 15 by sheriffbot on Wed, Mar 9, 2022, 1:02 PM EST Project Member

Labels: ReleaseBlock-Beta

This is a critical security issue. 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 16 by antrim@chromium.org on Wed, Mar 9, 2022, 1:06 PM EST Project Member

Owner: jopalmer@google.com
Cc: omrilio@chromium.org jopalmer@chromium.org shend@chromium.org

It seems that I've used outdated info in #13 to find engineer, re-assigning/adding other engineers to CC

Comment 17 by sheriffbot on Wed, Mar 9, 2022, 1:13 PM EST Project Member

Labels: -Pri-1 Pri-0

Setting Pri-0 to match security severity Critical. 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 18 by sheriffbot on Wed, Mar 9, 2022, 1:15 PM EST Project Member

Labels: ReleaseBlock-Urgent

This release blocker is now considered 'urgent' and therefore subject to the following SLOs:
Assigned Owner: 1 day
Comment SLO: Every day
Fix SLO: Within 3 days.

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

Comment 19 by kerrnel@google.com on Wed, Mar 9, 2022, 4:36 PM EST Project Member

Labels: -Security_Severity-Critical Security_Severity-High Pri-1

Comment 20 by kerrnel@google.com on Wed, Mar 9, 2022, 4:36 PM EST Project Member

Thanks for the reports, does ~~crbug.com/1300710~~ contain anything not in this report?

Comment 21 by jopalmer@google.com on Wed, Mar 9, 2022, 4:37 PM EST Project Member

investigating

Comment 22 by sheriffbot on Wed, Mar 9, 2022, 4:38 PM EST Project Member

Labels: Pri-0

This ReleaseBlock issue's priority is being increased in accordance with go/cros-bug-slo-guidelines#release-blockers.

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

Comment 23 by jopalmer@google.com on Wed, Mar 9, 2022, 4:53 PM EST Project Member

not reproing on HEAD - grabbing VK from that version to try to repro

Comment 24 by hesse...@googlemail.com on Wed, Mar 9, 2022, 5:04 PM EST

Hello,

~~Issue 1300710~~, better the following Issue 1303312 (with video proof) is showing how to manipulate the clipboard on locked devices, thus the "internals" of the locked session.

Here: Leak clipboard, there: Manipulate clipboard.

But these tickets were closed because they could not be reproduced, despite the video is demonstrating that it is possible. Unfortunately not every time, as I have to notice in the meantime.

Simply because it is a kind of related to the vulnerability handled here, investigated by your teams, I wanted to awake that other vulnerability just for one reason: Probably you notice the cause by the way/secondarily.

Comment 25 by jopalmer@google.com on Wed, Mar 9, 2022, 5:08 PM EST Project Member

I also fail to repro copying text from a VPN box showing up inside the logged in screen. I can't see 1303312. I suggest you follow up seperately with those bugs to keep this one focused on the current issue

Comment 26 by jopalmer@google.com on Wed, Mar 9, 2022, 5:08 PM EST Project Member

Cc: newcomer@chromium.org

Comment 27 by newcomer@chromium.org on Wed, Mar 9, 2022, 5:15 PM EST Project Member

Cc: -newcomer@chromium.org ckincaid@chromium.org mmourgos@chromium.org

I no longer own clipboard history. +ckincaid, current owner, and mmourgos@, who originally worked on the VK API.

IIRC, we don't show clipboard history via system UI in the lock screen, so we could fix this on either the VK side (don't show Clipboard History on the lock screen) or the API side (don't supply clipboard history data on the lock screen). Either should work given there is no caching on the VK side.

Comment 28 by jopalmer@google.com on Wed, Mar 9, 2022, 5:21 PM EST Project Member

Repro on M99

Comment 29 by shend@chromium.org on Wed, Mar 9, 2022, 5:23 PM EST Project Member

IMO fixing it on the API side seems more robust.

Comment 30 by ckincaid@chromium.org on Wed, Mar 9, 2022, 5:55 PM EST Project Member

Cc: jiwan@chromium.org

+jiwan@

I'm looking into fixing this on the API side. Can someone from the VK side confirm that the API results fetched with an unlocked screen will not be cached?

Comment 31 by jopalmer@google.com on Wed, Mar 9, 2022, 6:04 PM EST Project Member

Cc: dvallet@chromium.org

Comment 32 by jopalmer@google.com on Wed, Mar 9, 2022, 6:12 PM EST Project Member

VK at m99 is v_185

Comment 33 by jopalmer@google.com on Wed, Mar 9, 2022, 6:18 PM EST Project Member

My feeling is that there might be some caching on the VK side

Only repros if copy happens whilst in tablet mode when logged in (based on very quick testing)

Comment 34 by ckincaid@chromium.org on Wed, Mar 9, 2022, 6:21 PM EST Project Member

From my limited testing, it seems that in M101, the clipboard tab of VK is disabled when the screen is locked. Perhaps this is just because I populated the clipboard while in clamshell mode rather than tablet mode.

If this is the case, could we back-port the recent change that disables VK's clipboard access on locked screens? This would be in addition to the API-side fix.

Comment 35 by jopalmer@google.com on Wed, Mar 9, 2022, 6:26 PM EST Project Member

FYI: this still repros on HEAD - just missed some of the required steps to repro it

Comment 36 by jopalmer@google.com on Wed, Mar 9, 2022, 6:34 PM EST Project Member

Cc: shengjun@chromium.org

Comment 37 by jopalmer@google.com on Wed, Mar 9, 2022, 6:47 PM EST Project Member

Not completely caching - multipaste API is working at lock screen

verify via

```
 chrome.virtualKeyboardPrivate.getClipboardHistory({},(c)=> console.error(c))
```

Comment 38 by jopalmer@google.com on Wed, Mar 9, 2022, 6:55 PM EST Project Member

I think have a fix for the VK side.

going to get a few people to verify that it works fully. We are also planning on fixing the API side as well

Comment 39 by jopalmer@google.com on Wed, Mar 9, 2022, 6:56 PM EST Project Member

This bug has probably existed since around M94 or so

Comment 40 by ckincaid@chromium.org on Wed, Mar 9, 2022, 6:58 PM EST Project Member

Speculative fix for the API side at https://chromium-review.googlesource.com/c/chromium/src/+/3515152 if anyone wants to patch it in for verification. Will put it up for review if it passes CQ. Also going to try to add some automated testing in the meantime.

Comment 41 by jopalmer@google.com on Wed, Mar 9, 2022, 7:31 PM EST Project Member

Chatted to TPM and we have permission to land the VK fix in 99

Comment 42 by Git Watcher on Wed, Mar 9, 2022, 10:00 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/9bc07cd2ae189cd433e497a09424fdc3c52d2178

commit 9bc07cd2ae189cd433e497a09424fdc3c52d2178
Author: Colin Kincaid <ckincaid@chromium.org>
Date: Thu Mar 10 02:59:13 2022

Stop returning clipboard history to VK when screen is locked.

~~Bug: 1303410~~
Change-Id: I0df4d2af2d7856b0e8c588b3893c8b9c86c99ad9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3515152
Reviewed-by: Darren Shen <shend@chromium.org>
Commit-Queue: Colin Kincaid <ckincaid@chromium.org>
Cr-Commit-Position: refs/heads/main@{#979611}

[modify]
https://crrev.com/9bc07cd2ae189cd433e497a09424fdc3c52d2178/chrome/browser/extensions/api/virtual_keyboard_privat

e/chrome_virtual_keyboard_delegate.cc
[modify]
https://crrev.com/9bc07cd2ae189cd433e497a09424fdc3c52d2178/chrome/test/data/extensions/api_test/virtual_keyboard_private/test.js
[modify]
https://crrev.com/9bc07cd2ae189cd433e497a09424fdc3c52d2178/chrome/browser/extensions/api/virtual_keyboard_private/virtual_keyboard_private_apitest.cc

Comment 43 by Git Watcher on Wed, Mar 9, 2022, 10:12 PM EST Project Member

Labels: merge-merged-release-R99-14469.B

The following revision refers to this bug:
https://chrome-internal.googlesource.com/chromeos/overlays/chromeos-overlay/+/2aa57795821ed4f99b33759e78d00b522e2a9029

commit 2aa57795821ed4f99b33759e78d00b522e2a9029
Author: John Palmer <jopalmer@google.com>
Date: Thu Mar 10 02:50:35 2022

Comment 44 by ckincaid@chromium.org on Wed, Mar 9, 2022, 10:15 PM EST Project Member

Labels: Self-Merge-Request-99 Merge-Request-100

Cannot repro issue with Multipaste API fix above. Will merge into M99 and M100.

Comment 45 by sheriffbot on Wed, Mar 9, 2022, 10:20 PM EST Project Member

Labels: -Self-Merge-Request-99 Merge-Review-99

This bug was flagged as a self-merge request.

As part of Chrome OS' transition to a 4-week release cycle, self-merges have been deprecated. This merge request will need to be reviewed and approved by a Release TPgM in order to be merged to a release branch. Please review http://goto.google.com/cros-merge-guidelines and ensure that this request meets the requirements for review. We've added the Merge-Review-99 label and removed the self-merge label to this bug. Please ensure the following questions are answered so this request can be reviewed:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?
8. Has your Eng Prod Representative approved (in any form) that testing for this change can be accommodated? (if this merge would change/add to the required testing)
- See http://go/cros-engprodcomponents to find your representative (if you do not have access, please work with your Google contact)

Please contact the milestone owner if you have questions.

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

Comment 46 by jopalmer@google.com on Wed, Mar 9, 2022, 10:24 PM EST Project Member

Some quick notes to clarify where we are

Repro steps:
1) Add a VPN (os settings > network > add VPN) (just add enough stuff for create to work, doesn't need to be a functioning VPN)
2) In TABLET MODE copy some text + show Virtual keyboard to verify that multipaste suggestion shows in a new empty text field
3) Lock screen
4) Use shelf to open VPN settings and get the VPN popup
5) Open vitual keyboard on one of the text fields
6) observe clipboard contents present

Note that (6) needs to be done within 2 minutes of (2) due to how the multipaste feature works in the VK.
There may be other ways to repro this at the lock screen, but we have not investigated.

Fix on virtual keyboard side has landed on M99 (via https://chrome-internal-review.googlesource.com/c/chromeos/overlays/chromeos-overlay/+/4603194), I think it missed today's respin so should go out in the next one. Still need a virtual keyboard fix for M100 but that should happen shortly

Comment 47 by ckincaid@chromium.org on Wed, Mar 9, 2022, 10:29 PM EST Project Member

Cc: dhadd...@chromium.org
Components: UI>Shell>EnhancedClipboard

1. Yes, this is a medium-severity security issue (information leak)
2. https://chromium-review.googlesource.com/c/chromium/src/+/3515152
3. Yes
4. M99 and M100
5. Security issue
6. No
7. N/A
8. +dhaddock@

Comment 48 by jopalmer@google.com on Wed, Mar 9, 2022, 11:05 PM EST Project Member

For the VK side as above except for (2) we have cl/433607788

VK fix already landed on M99, but not yet for M100 after chatting to ceb@

Comment 49 by hesse...@googlemail.com on Thu, Mar 10, 2022, 3:37 AM EST

Hello together, I extracted side note #2 from the initial report now to a new ticket, ~~Issue 1305117~~.

Comment 50 by kerrnel@google.com on Thu, Mar 10, 2022, 12:09 PM EST Project Member

Labels: Pri-1

What is side note #2? Please try not to file multiple tickets about the same bug as it confuses our attempts to address this.

Comment 51 by kerrnel@google.com on Thu, Mar 10, 2022, 12:10 PM EST Project Member

Cc: kerrnel@chromium.org

Comment 52 by sheriffbot on Thu, Mar 10, 2022, 12:19 PM EST Project Member

Labels: Pri-0

This ReleaseBlock issue's priority is being increased in accordance with go/cros-bug-slo-guidelines#release-blockers.

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

Comment 53 by dgagnon@google.com on Thu, Mar 10, 2022, 6:51 PM EST Project Member

Labels: -Merge-Request-100 Merge-Approved-100

If no issues from dhaddock@, merge approved for M100

Comment 54 by dhadd...@chromium.org on Thu, Mar 10, 2022, 6:57 PM EST Project Member

LGTM

Comment 55 by ckincaid@chromium.org on Thu, Mar 10, 2022, 7:06 PM EST Project Member

Thanks! Pending approval from dmblack@, I'd also like to merge https://chromium-review.googlesource.com/c/chromium/src/+/3517909 to M99 and M100.

Comment 56 by bookholt@chromium.org on Thu, Mar 10, 2022, 7:24 PM EST Project Member

~~Issue 1305117~~ has been merged into this issue.

Comment 57 by dcheng@chromium.org on Thu, Mar 10, 2022, 7:39 PM EST Project Member

Just to be clear, does the VK also prevent predictions/suggestions from crossing session boundaries?

Comment 58 by jopalmer@google.com on Sun, Mar 13, 2022, 7:26 PM EDT Project Member

Predictions should also be scoped to user sessions (relevant files are stored in user home dir I believe)

Comment 59 by antrim@chromium.org on Mon, Mar 14, 2022, 8:19 AM EDT Project Member

The problem with locked session is that user home dir is still accessible, so if scoping logic is based only on the access to the data, it would not prevent leak.

Comment 60 by sheriffbot on Mon, Mar 14, 2022, 12:24 PM EDT Project Member

Cc: dgagnon@google.com

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 61 by ceb@google.com on Mon, Mar 14, 2022, 2:46 PM EDT Project Member

Merge approved for M99.

Comment 62 by ceb@google.com on Mon, Mar 14, 2022, 2:46 PM EDT Project Member

Labels: -Merge-Review-99 M-100 Merge-Approved-99

Comment 63 by dcheng@chromium.org on Mon, Mar 14, 2022, 2:58 PM EDT Project Member

> The problem with locked session is that user home dir is still accessible, so if scoping logic is based only on the access to the data, it would not prevent leak.

Does this mean we need another followup for personalization leaks?

Comment 64 by jopalmer@google.com on Mon, Mar 14, 2022, 5:45 PM EDT Project Member

We are checking if personalised suggestions also leak at the lock screen manually as well. Initial results seem to suggest NO.

Comment 65 by Git Watcher on Mon, Mar 14, 2022, 6:12 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/+/63bf63f82948b30112eb38f5f0d128141b88386f

commit 63bf63f82948b30112eb38f5f0d128141b88386f
Author: Colin Kincaid <ckincaid@chromium.org>
Date: Mon Mar 14 22:11:45 2022

Stop returning clipboard history to VK when screen is locked.

(cherry picked from commit 9bc07cd2ae189cd433e497a09424fdc3c52d2178)

~~Bug: 1303410~~
Change-Id: I0df4d2af2d7856b0e8c588b3893c8b9c86c99ad9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3515152
Reviewed-by: Darren Shen <shend@chromium.org>
Commit-Queue: Colin Kincaid <ckincaid@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#979611}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3517006
Auto-Submit: Colin Kincaid <ckincaid@chromium.org>
Commit-Queue: Darren Shen <shend@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#536}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/63bf63f82948b30112eb38f5f0d128141b88386f/chrome/browser/extensions/api/virtual_keyboard_private/chrome_virtual_keyboard_delegate.cc
[modify]
https://crrev.com/63bf63f82948b30112eb38f5f0d128141b88386f/chrome/test/data/extensions/api_test/virtual_keyboard_private/test.js
[modify]
https://crrev.com/63bf63f82948b30112eb38f5f0d128141b88386f/chrome/browser/extensions/api/virtual_keyboard_private/virtual_keyboard_private_apitest.cc

Comment 66 by Git Watcher on Mon, Mar 14, 2022, 6:17 PM EDT Project Member

Labels: -merge-approved-99 merge-merged-4844 merge-merged-99

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/35e6332614f84ac4acf053e54b9378e92703bc36

commit 35e6332614f84ac4acf053e54b9378e92703bc36
Author: Colin Kincaid <ckincaid@chromium.org>
Date: Mon Mar 14 22:16:39 2022

Stop returning clipboard history to VK when screen is locked.

(cherry picked from commit 9bc07cd2ae189cd433e497a09424fdc3c52d2178)

~~Bug: 1303410~~
Change-Id: I0df4d2af2d7856b0e8c588b3893c8b9c86c99ad9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3515152
Reviewed-by: Darren Shen <shend@chromium.org>
Commit-Queue: Colin Kincaid <ckincaid@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#979611}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3518489
Auto-Submit: Colin Kincaid <ckincaid@chromium.org>
Commit-Queue: Darren Shen <shend@chromium.org>
Cr-Commit-Position: refs/branch-heads/4844@{#1061}
Cr-Branched-From: 007241ce2e6c8e5a7b306cc36c730cd07cd38825-refs/heads/main@{#961656}

[modify]
https://crrev.com/35e6332614f84ac4acf053e54b9378e92703bc36/chrome/browser/extensions/api/virtual_keyboard_private/chrome_virtual_keyboard_delegate.cc
[modify]
https://crrev.com/35e6332614f84ac4acf053e54b9378e92703bc36/chrome/test/data/extensions/api_test/virtual_keyboard_private/test.js
[modify]
https://crrev.com/35e6332614f84ac4acf053e54b9378e92703bc36/chrome/browser/extensions/api/virtual_keyboard_private/virtual_keyboard_private_apitest.cc

Comment 67 by gmpritchard@google.com on Tue, Mar 15, 2022, 12:33 PM EDT Project Member

Cc: gmpritchard@google.com

Comment 68 by gmpritchard@google.com on Tue, Mar 15, 2022, 2:04 PM EDT Project Member

Should this bug be marked fixed? ckincaid@

Comment 69 by ckincaid@chromium.org on Tue, Mar 15, 2022, 2:14 PM EDT Project Member

I believe so, but I'll let jopalmer@ confirm. Not sure if there's further follow-up to do on the VK side wrt personalized suggestions.

Comment 70 by jopalmer@google.com on Tue, Mar 15, 2022, 5:40 PM EDT Project Member

VK hasn't landed on m100 yet, hopefully we land today

Comment 71 by jopalmer@google.com on Wed, Mar 16, 2022, 6:04 PM EDT Project Member

Status: Fixed (was: Assigned)

M100 landed for the VK now

Comment 72 by sheriffbot on Wed, Mar 16, 2022, 6:05 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 73 by jopalmer@google.com on Wed, Mar 16, 2022, 7:55 PM EDT Project Member

Status: Assigned (was: Fixed)

1) no
2) Possibly?

Reopening to verify on m96

Comment 74 by jopalmer@google.com on Wed, Mar 16, 2022, 8:35 PM EDT Project Member

Status: Fixed (was: Assigned)

Bug is behind a flag which is default off in M96, so closing again

Comment 75 by hesse...@googlemail.com on Thu, Mar 17, 2022, 5:47 AM EDT

Hi, I see that the issue was marked as "fixed". May I kindly ask you how the behaviour (leak) from #56 will be handled?

Comment 76 by gmpritchard@google.com on Thu, Mar 17, 2022, 10:10 AM EDT Project Member

Labels: -LTS-Merge-Candidate LTS-NotApplicable-96

Comment 77 by rzanoni@google.com on Thu, Mar 17, 2022, 10:10 AM EDT Project Member

Labels: LTS-Evaluating-96

Comment 78 by rzanoni@google.com on Thu, Mar 17, 2022, 10:16 AM EDT Project Member

Labels: -LTS-NotApplicable-96

Comment 79 by rzanoni@google.com on Thu, Mar 17, 2022, 10:16 AM EDT Project Member

Labels: -LTS-Evaluating-96 LTS-NotApplicable-96

Comment 80 by sheriffbot on Thu, Mar 17, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 81 by sheriffbot on Thu, Mar 17, 2022, 1:42 PM EDT Project Member

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

Comment 82 by hesse...@googlemail.com on Wed, Mar 23, 2022, 6:59 PM EDT

Hello jopalmer@,

May I kindly ask you how the behaviour (leak) from #56 will be handled, what the final assessment is?

Comment 83 by jopalmer@google.com on Wed, Mar 23, 2022, 7:02 PM EDT Project Member

I can't see ~~crbug.com/1305117~~

Comment 84 by hesse...@googlemail.com on Wed, Mar 23, 2022, 7:06 PM EDT

It's side note no. 2 from the initial report in this ticket, extracted to 1305117, because it was obviously missed here.

Comment 85 by jopalmer@google.com on Wed, Mar 23, 2022, 7:11 PM EDT Project Member

Oh - we just don't display the suggestion from multipaste any more

Comment 86 by dcheng@chromium.org on Wed, Mar 23, 2022, 7:15 PM EDT Project Member

To clarify, I believe that it's about personalized suggestions from the keyboard, which I think is probably distinct from suggestions from multipaste? I asked about this in https://bugs.chromium.org/p/chromium/issues/detail?id=1303410#c63, and I think the reply was that this should be OK, but reading the replies again, I'm not sure if this is referring to personalized suggestions in the keyboard itself, or suggestions in the keyboard due to multipaste.

Comment 87 by dcheng@chromium.org on Wed, Mar 23, 2022, 7:18 PM EDT Project Member

For the reporter, your contributions are appreciated, but I suggest not filing so many bugs: since the discussion has forked into multiple different bugs, it's getting quite hard to keep track of if there are outstanding issues, and it's also becoming increasingly unclear to those who are triaging bugs if bugs are dupes or not.

Even if bugs are closed/marked as fixed, it's useful to try to have one central discussion somewhere, and mark any additional bugs as blockers.

Comment 88 by jopalmer@google.com on Wed, Mar 23, 2022, 7:42 PM EDT Project Member

Non multipaste suggestions are also getting disabled, but not due to this bug (found after testing by QA separately)

Hard to keep track with so many comments in different bugs + multipaste seemed main focus here

Comment 89 by jopalmer@google.com on Wed, Mar 23, 2022, 11:33 PM EDT Project Member

Components: UI>Input>VirtualKeyboard

Comment 90 by hesse...@googlemail.com on Thu, Mar 24, 2022, 2:02 AM EDT

That was the reason why I extracted it to the separate ticket.:)
The main thing is to get rid of the suggestions. May you set the ticket's ~~crbug.com/1305117~~ status to "fixed" afterwards? Would be great.

Comment 91 by kerrnel@google.com on Thu, Mar 24, 2022, 11:48 AM EDT Project Member

If they did the fix in this bug, it makes sense for ~~crbug.com/1305117~~ to be a duplicate, please trust the team's bug routing process, as mentioned it's making it very difficult to have a clear discussion about this. Too many bugs and different threads. :-)

Comment 92 by jopalmer@google.com on Thu, Mar 24, 2022, 5:47 PM EDT Project Member

I can't see ~~crbug.com/1305117~~ so I can't verify if we have fixed it / plan to fix it

Comment 93 by amyressler@chromium.org on Mon, Mar 28, 2022, 5:40 PM EDT Project Member

Labels: Release-0-M100

Comment 94 by amyressler@chromium.org on Tue, Mar 29, 2022, 12:25 PM EDT Project Member

Hello, reporter -- how would you like to be acknowledged for this issue. Please provide the name, tag, or other identifier you would like us to use in acknowledging you for this issue. Thank you.

Comment 95 by amyressler@google.com on Tue, Mar 29, 2022, 1:14 PM EDT Project Member

Labels: CVE-2022-1132 CVE_description-missing

Comment 96 by amyressler@google.com on Thu, Mar 31, 2022, 5:14 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** 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 97 by amyressler@chromium.org on Thu, Mar 31, 2022, 5:21 PM EDT Project Member

Congratulations! After evaluating this report and the security impact of this bug, the VRP Panel has decided to award you $5000 for this report. As this is a lockscreen bypass, it is relegated to accessing the clipboard contents only. A member of our finance team will be in touch within the coming days to arrange for payment systems enrollment and payment. Thank you for your efforts and reporting this issue to us.

Comment 98 by amyressler@google.com on Fri, Apr 1, 2022, 4:03 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 99 by sheriffbot on Thu, Jun 23, 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 100 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 101 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing

Comment 102 by bug-syncer on Mon, Nov 7, 2022, 7:47 PM EST (18 days ago) Project Member

Labels: Restrict-AddIssueComment-scr2b-migration migrated-to-b-258075040

Migrated to https://issuetracker.google.com/issues/258075040

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy