☆ Starred by 2 users

Owner:	sammiequon@chromium.org
CC:	sammiequon@chromium.org xiaoyinh@chromium.org khorimoto@chromium.org hllee@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Shell>Fingerprint
Modified:	Dec 22, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Chrome
Pri:	1
Type:	Bug-Security

reward-10000
Security_Severity-Medium
Arch-x86_64
Hotlist-Merge-Approved
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
M-95
FoundIn-92
Security_Impact-Extended
Release-0-M96
CVE-2021-38013
Proj-Fingerprints

Issue 1242392: heap buffer overflow iin FingerprintHandler::HandleGetEnrollmentLabel

Reported by wxhu...@gmail.com on Mon, Aug 23, 2021, 9:54 AM EDT

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36

Steps to reproduce the problem:
in the function chromeos::settings::FingerprintHandler::HandleGetEnrollmentLabel

the varibale of index could be defined by js as below.

```
<script>
  var arr1 = ["test", 12314];
  chrome.send("getEnrollmentLabel", arr1);
</script>
```

it will cause heap bufferoverlow, but when the index is larger then 2, the stack trace will show heap use after free.

it is strange, if someone have a uxss in chromium, then he may use these code to get command execute.

I patch the function chromeos::settings::FingerprintHandler::HandleGetEnrollmentLabel that makes the variable of fingerprints_paths is not null, the fingerprints_paths in my linux-chromeos is null that causs null pointer, but I think in real device ,it could be not null,

how to trigger?

- in chromeos version open the settings, inspect the window, and enter the js, than it will crash.

What is the expected behavior?

What went wrong?
above all

Did this work before? N/A

Chrome version: 92.0.4515.159 Channel: stable
OS Version: 10.0

heap_buffer_overflow.txt
13.8 KB View Download

image-20210823214552973.png
81.1 KB View Download

Comment 1 by wxhu...@gmail.com on Mon, Aug 23, 2021, 9:56 AM EDT

the other function like 'FingerprintHandler::HandleRemoveEnrollment' and 'FingerprintHandler::HandleChangeEnrollmentLabel' has the same vul.

Comment 2 by wxhu...@gmail.com on Mon, Aug 23, 2021, 9:57 AM EDT

the fix is easy, before use the index, we should check the bound of index

Comment 3 by sheriffbot on Mon, Aug 23, 2021, 10:00 AM EDT

Labels: external_security_report

Comment 4 by wxhu...@gmail.com on Mon, Aug 23, 2021, 11:09 AM EDT

Can I split this bug to three bug as your policy?

Comment 5 by wxhu...@gmail.com on Wed, Aug 25, 2021, 12:16 AM EDT

I have submit two issue to track there overflow problems.
~~issue 1243165~~. and ~~issue 1243166~~
If your policy think these issue is the same, feel free to merge into this one.

Comment 6 Deleted

Comment 7 Deleted

Comment 8 by wxhu...@gmail.com on Wed, Aug 25, 2021, 12:34 AM EDT

0001-fix-heap-bufferoverflow-in-fingerprint_handler.patch
1.8 KB View Download

Comment 9 by wxhu...@gmail.com on Wed, Aug 25, 2021, 1:21 PM EDT

from the code, this only can be trigger in chromeos version.

Comment 10 by drubery@chromium.org on Wed, Aug 25, 2021, 4:00 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: sammiequon@chromium.org
Cc: xiaoyinh@chromium.org
Labels: -OS-Windows Security_Severity-Medium FoundIn-92 OS-Chrome
Components: UI>Shell>Fingerprint

This does reproduce (though I notice there's a DCHECK that triggers in these conditions). Triaging to a fingerprint OWNER and assigning Medium severity since it would require the ability to inject JS to chrome://settings.

Comment 11 by sheriffbot on Wed, Aug 25, 2021, 4:00 PM EDT

Labels: Security_Impact-Extended

Comment 12 by jorgelo@chromium.org on Wed, Aug 25, 2021, 5:23 PM EDT

Labels: M-95

Comment 13 by sheriffbot on Thu, Aug 26, 2021, 1:17 PM EDT

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 14 Deleted

Comment 15 by sheriffbot on Mon, Sep 6, 2021, 12:21 PM EDT

sammiequon: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

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 16 by wxhu...@gmail.com on Wed, Sep 8, 2021, 10:58 PM EDT

here is the patch

0001-fix-heap-overflow-in-fingerprint.patch
1.8 KB View Download

Comment 17 by sammiequon@chromium.org on Fri, Sep 10, 2021, 12:03 PM EDT

Cc: khorimoto@chromium.org

Comment 18 by Git Watcher on Mon, Sep 13, 2021, 4:17 PM EDT

Status: Fixed (was: Assigned)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/57def0f4c02587a7758edde865de044336193185

commit 57def0f4c02587a7758edde865de044336193185
Author: Sammie Quon <sammiequon@chromium.org>
Date: Fri Sep 10 17:33:20 2021

cros: Fix security issue with fingerprint settings APIs.

Change some DCHECKs to CHECKs which is the pattern used by other
settings pages.

Test: manual
~~Fixed: 1242392~~, ~~1243165~~, ~~1243166~~
Change-Id: Ia816b8a046fb4c0f69e76c79cbe2043005a1a9a7
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3152181
Reviewed-by: Kyle Horimoto <khorimoto@chromium.org>
Commit-Queue: Sammie Quon <sammiequon@chromium.org>
Cr-Commit-Position: refs/heads/main@{#920270}

[modify] https://crrev.com/57def0f4c02587a7758edde865de044336193185/chrome/browser/ui/webui/settings/chromeos/fingerprint_handler.cc

Comment 19 by sheriffbot on Tue, Sep 14, 2021, 12:42 PM EDT

Labels: reward-topanel

Comment 20 by sheriffbot on Tue, Sep 14, 2021, 1:42 PM EDT

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

Comment 21 by sheriffbot on Tue, Sep 14, 2021, 2:13 PM EDT

Labels: Merge-Request-95

Requesting merge to dev M95 because latest trunk commit (920270) appears to be after dev branch point (920003).

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

Comment 22 by sheriffbot on Wed, Sep 15, 2021, 2:16 PM EDT

Labels: -Merge-Request-95 Hotlist-Merge-Approved Merge-Approved-95

Your change meets the bar and is auto-approved for M95. Please go ahead and merge the CL to branch 4638 (refs/branch-heads/4638) manually. Please contact milestone owner if you have questions.
Merge instructions: https://www.chromium.org/developers/how-tos/drover
Owners: benmason@(Android), harrysouders@(iOS), None@(ChromeOS), pbommana@(Desktop)

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

Comment 23 by sheriffbot on Mon, Sep 20, 2021, 12:19 PM EDT

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 24 by khorimoto@chromium.org on Mon, Sep 20, 2021, 12:22 PM EDT

Labels: -Merge-Approved-95

Not merging to M-95 since it is skipped for Chrome OS.

Comment 25 by amyressler@chromium.org on Wed, Sep 22, 2021, 3:19 PM EDT

Cc: sammiequon@chromium.org

~~Issue 1243165~~ has been merged into this issue.

Comment 26 by amyressler@chromium.org on Wed, Sep 22, 2021, 3:20 PM EDT

~~Issue 1243166~~ has been merged into this issue.

Comment 27 by amyressler@google.com on Thu, Sep 30, 2021, 10:30 AM EDT

Labels: -reward-topanel reward-unpaid reward-10000

*** 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 28 by wxhu...@gmail.com on Thu, Sep 30, 2021, 10:34 AM EDT

Thank you.

Comment 29 by amyressler@chromium.org on Thu, Sep 30, 2021, 12:32 PM EDT

Congratulations and great finding!

Comment 30 by amyressler@google.com on Fri, Oct 1, 2021, 11:34 AM EDT

Labels: -reward-unpaid reward-inprocess

Comment 31 by amyressler@chromium.org on Thu, Nov 11, 2021, 5:54 PM EST

Labels: Release-0-M96

(Sheriffbot didn't ask for merges here. That Sheriffbot bug is tracked as issue 1262390).

Comment 32 by adetaylor@google.com on Thu, Nov 11, 2021, 7:05 PM EST

Labels: CVE-2021-38013 CVE_description-missing

Comment 33 by sheriffbot on Tue, Dec 21, 2021, 1:29 PM EST

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 34 by amyressler@google.com on Wed, Dec 22, 2021, 7:11 PM EST

Labels: -CVE_description-missing CVE_description-submitted