☆ Starred by 3 users

| | |
|---|---|
| **Owner:** | rouslan@chromium.org |
| **CC:** | adetaylor@chromium.org<br>maxlg@chromium.org |
| **Status:** | Fixed *(Closed)* |
| **Components:** | Blink>Payments |
| **Modified:** | Jun 24, 2021 |
| **Backlog-Rank:** | ---- |
| **Editors:** | ---- |
| **EstimatedDays:** | ---- |
| **NextAction:** | ---- |
| **OS:** | Android |
| **Pri:** | 2 |
| **Type:** | Bug-Security |

reward-500
Security_Severity-Low
Security_Impact-Stable
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
external_security_bug
Release-0-M91
CVE-2021-30540

## Issue 1184147: Security: Incorrect Security UI in payment

Reported by zyzen...@gmail.com on Wed, Mar 3, 2021, 4:43 AM EST

Code

Steps to reproduce the problem:
1.open "https://lightrains.org/js/poc/evil.html" in android chrome

2.click link “Install Google Pay Web Payment App”

3.then open "https://rsolomakhin.github.io/pr/contact/" in another tab

you will see crlf code has been injection into the payment handler

What is the expected behavior?

What went wrong?
CRLF code injection via payment manifest

https://github.com/We5ter/We5ter.github.io/blob/master/js/pay/manifest.json

Did this work before? N/A

Chrome version: 89.0.4370.0 Channel: n/a
OS Version:
Flash Version:

[Deleted] **poc_payment.jpg**

Comment 1 by sheriffbot on Wed, Mar 3, 2021, 4:47 AM EST

**Labels:** external_security_report

Comment 2 by zyzen...@gmail.com on Wed, Mar 3, 2021, 7:32 AM EST

[Deleted] **poc_payment2.jpg**

Comment 3 by dominickn@chromium.org on Wed, Mar 3, 2021, 5:58 PM EST

**Status:** Assigned (was: Unconfirmed)
**Owner:** rouslan@chromium.org
**Cc:** maxlg@chromium.org
**Components:** Blink>Payments

+rouslan, do you mind taking a look at this and commenting on whether there is an issue here?

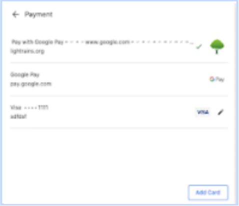
Comment 4 by rouslan@chromium.org on Thu, Mar 4, 2021, 9:22 AM EST

This is an issue that is hard to prevent in 100% of cases. The name of the payment app is defined in web app manifest (https://lightrains.org/js/pay/manifest.json in this instance). It could be "www.google.com", "paypal.com", or "amazon.com" and we don't check for that. For service worker based payment apps, we do show the URL of the app next to the app name, so making the app name single-line in Android UI should improve the situation. However, note that desktop UI has this single-line property and it's not immediately clear to the user why there're two URLs in the payment app name (see the attached screenshot).

Once the user has launched the payment app in the bottom sheet, that bottom sheet displays the URL of the payment app as well. The title of the payment app in that case is correctly set to be single line (see the attached screenshot).

Next steps (Rouslan): I will send out a patch to make the app name in the PaymentRequest Android UI into a single line.

**Screen Shot 2021-03-04 at 9.08.26 AM.png**
26.7 KB View Download



Payment

Pay with Google Pay - - - - www.google.com - - - - - - - - - - -...
lightrains.org

Google Pay
pay.google.com

Visa ····1111
adfdsf

Add Card

**Screenshot_20210304-091826.png**
156 KB View Download

Contact details

Comment 5 by dominickn@chromium.org on Thu, Mar 4, 2021, 4:36 PM EST
**Labels:** Security_Impact-Stable Security_Severity-Low

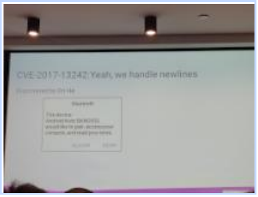
Thanks Rouslan, I'll assign security labels per your response. :)

Comment 6 Deleted

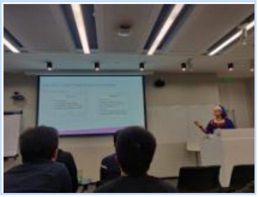
Comment 7 by zyzen...@gmail.com on Thu, Mar 4, 2021, 10:23 PM EST

And also my friend En He report a same case for injecting newline code into Android OS bluetooth pair dialog box, it's also just inject some text into dialog to change the original sentences meanings, AOSP security team treat this as high severity and reward $6000, so as the same, payment is the most important function of chrome, security and privacy of UI is extremely important.

**aosp1.jpg**
4.7 MB View Download



**aosp2.jpg**
6.0 MB View Download



**aosp3.jpg**
5.4 MB View Download

Comment 8 by zyzen...@gmail.com on Thu, Mar 4, 2021, 10:25 PM EST

severity need to upgrade

Comment 9 by Git Watcher on Fri, Mar 5, 2021, 10:53 AM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ae2f3eb465c5786729e26c6d4a1cdc32c0159cc8

commit ae2f3eb465c5786729e26c6d4a1cdc32c0159cc8
Author: Rouslan Solomakhin <rouslan@chromium.org>
Date: Fri Mar 05 15:52:46 2021

[Web Payment] Remove line terminators from payment app label.

Before this patch, the payment app name with newlines and carriage
returns could be displayed in the Android payment app chooser in

multiple lines, which would push the origin (URL) of the payment app
lower. A malicious payment app could use this to attempt to spoof its
origin.

This patch removes "\r", "\f", "\n", "\u0085", "\u2028", and "\u2029"
line terminators from the labels of the payment app base class on
Android, which is used by the service worker and Android payment apps.

The user interface uses newlines to combine multiple pieces of
information, which is especially useful for shipping addresses and
contact information. The same user interface is also used by Autofill
assistant. Therefore, making the UI use a single line for all labels
requires a more involved solution.

After this patch, PaymentRequest payment apps (service worker and
Android apps) cannot use line terminators in their name to show
multi-line app names.

~~Bug: 1184147~~
Change-Id: Ia4e4e8fc4d6467f438d265015e13d91d2ac3bf85
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2736000
Reviewed-by: Liquan (Max) Gu <maxlg@chromium.org>
Commit-Queue: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Commit-Position: refs/heads/master@{#860249}

[modify]
https://crrev.com/ae2f3eb465c5786729e26c6d4a1cdc32c0159cc8/components/payments/content/android/java/src/org/chromium/components/payments/PaymentApp.java

Comment 10 by rouslan@google.com on Fri, Mar 5, 2021, 1:49 PM EST

We plan to stop using this payment UI surface in 2021. There's a feature to skip that UI surface to go directly into the payment apps and we're seeing way more usage of the skip-UI flow. It's possible that this UI surface will be replaced with a simplified app chooser UI, similar to Android's "Share" dialog. As such and in addition to the reasoning stated in the patch description, I'm reluctant to invest time into the more involved solution of making the UI use a single line for all labels.

I will mark this bug report fixed after I verify the fix on Canary.

Dom: Does this patch require a merge into any of the branches, given that it's marked low severity?

Comment 11 by dominickn@chromium.org on Fri, Mar 5, 2021, 6:12 PM EST

#7: the URL bar is Chrome's trusted area for showing the origin. That is showing the correct URL in this case ("lightrains.org"). If this issue was able to change the URL in the URL bar when the payment app is shown for confirmation of purchase, then it would be higher severity.

#10: usually we don't merge fixes for low security bugs, but once this is fixed the security TPM should come by to confirm. Thanks for the quick investigation! :)

Comment 12 by zyzen...@gmail.com on Fri, Mar 5, 2021, 6:39 PM EST

Thanks, as you said, I changed the domain name to pay.google.com, on the payment pop-up page and told him through sentences semantics that we would use a backup site such as googlepay-backup.com, even though the address bar shows googlepay-backup.com in the next steps. Can the vast majority of ordinary users know that this is a fake? I don't think so. They don't know that the googlepay domain name must be pay.google.com rather than anything else. They will choose to believe the description of chrome.

Comment 13 by zyzen...@gmail.com on Fri, Mar 5, 2021, 6:42 PM EST

Another newline code injection case(#1180126) I reported in web app install is severity high.

Comment 14 by dominickn@chromium.org on Fri, Mar 5, 2021, 9:59 PM EST

#12: your description seems akin to someone creating a webpage which is a complete clone of Amazon except for the URL in the URL bar. The web can put any content it likes in the content - by design. Browsers - by design - do not control the content in the web content area. We use the security UI like the URL bar to prove the identity of content.

Issue 1180126 is completely different to this issue because the attack completely hides the origin in the install UI and replaces it. This attack does not prevent the trusted UI (the URL bar) from being seen and does not make that trusted UI show incorrect data.

Comment 15 by zyzen...@gmail.com on Sat, Mar 6, 2021, 3:29 AM EST

Alright, it's fine, thanks for your detail reply @Dominickn, could you consider to upgrade its bounty because it is payment API? not $500 again.

Comment 16 by rouslan@google.com on Mon, Mar 8, 2021, 7:30 AM EST

The name of the payment app wraps, so I think an ellipsis after around 30 characters could be a good idea. I'm not aware of any legitimate payment apps whose names are longer than that, but I will send out a newsletter to paymentrequest@chromium.org to give a heads up.

Comment 17 by rouslan@google.com on Mon, Mar 8, 2021, 7:30 AM EST

**Screenshot_20210308-072721.png**
285 KB View Download

Credit Card Test

Comment 18 by sheriffbot on Wed, Mar 10, 2021, 8:03 PM EST

**Labels:** reward-potential

Comment 19 by Git Watcher on Fri, Mar 12, 2021, 3:57 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b624be2c0199f5284458c737e08eba7d15d5a730

commit b624be2c0199f5284458c737e08eba7d15d5a730
Author: Rouslan Solomakhin <rouslan@chromium.org>
Date: Fri Mar 12 20:56:22 2021

[Web Payment] Elide payment app name on Android

Before this patch, Android payment app chooser could wrap a long payment
app name, which could be confusing to the user, because the second line
can be used to show the origin of a service worker based payment app.

This patch truncates the payment app name in the payment app base class
on Android to 64 characters. If a name is longer than that, then a
unicode horizontal ellipsis is appended to the name.

The user interface uses newlines and text wrapping to combine
multiple pieces of information, which is especially useful for
shipping addresses and contact information. The same user interface
is also used by Autofill assistant. Therefore, making the UI use
a single line with OS controlled ellison for all labels requires
a more involved solution. In addition, we plan to stop using this
particular UI surface as a payment app chooser this year.
The upcoming replacement UI should use a single line for
website-defined names, so the elision can be taken care of by
the Android OS.

After this patch, the maximum length of a payment app name in the
Android payment app chooser is 64 characters. Longer names are elided.

~~Bug: 1184147~~
Change-Id: I455db5878ce8e28e22ca1fa276d6da621a9f67f6
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2743334
Commit-Queue: Rouslan Solomakhin <rouslan@chromium.org>
Reviewed-by: Liquan (Max) Gu <maxlg@chromium.org>
Cr-Commit-Position: refs/heads/master@{#862517}

[modify]
https://crrev.com/b624be2c0199f5284458c737e08eba7d15d5a730/components/payments/content/android/java/src/org/chromium/components/payments/PaymentApp.java

Comment 20 by rouslan@google.com on Mon, Mar 15, 2021, 10:51 AM EDT
**Cc:** adetaylor@chromium.org

cc += adetaylor@ - could you please confirm that this bug fix does not need to be merged into release branches?

Comment 21 by adetaylor@chromium.org on Mon, Mar 15, 2021, 11:01 AM EDT

Hi, in general please mark the bug as Fixed and sheriffbot will take care of merge labels:
https://chromium.googlesource.com/chromium/src/+/master/docs/security/security-labels.md#TOC-Merge-labels
But in this specific case - for a Low bug - no merge is needed. Thanks for the fix.

Comment 22 by rouslan@google.com on Mon, Mar 15, 2021, 12:38 PM EDT
**Status:** Fixed (was: Assigned)

Great to know, thank you!!!

Comment 23 by sheriffbot on Mon, Mar 15, 2021, 12:42 PM EDT
**Labels:** reward-topanel

Comment 24 by sheriffbot on Mon, Mar 15, 2021, 1:56 PM EDT
**Labels:** -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 25 by zhangtiff@google.com on Wed, Mar 17, 2021, 7:14 PM EDT
**Labels:** -reward-potential external_security_bug

Comment 26 by amyressler@google.com on Wed, Mar 31, 2021, 6:20 PM EDT
**Labels:** -reward-topanel reward-unpaid reward-500

*** 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 27 by amyressler@google.com on Wed, Mar 31, 2021, 7:36 PM EDT

Hello zyzengstorm@, the VRP Panel has decided to award you $500 for this report. Thank you for your efforts!

Comment 28 by zyzen...@gmail.com on Wed, Mar 31, 2021, 9:53 PM EDT

ALright, but payment is an api more important than share or tap preview(my ~~bug #1133183~~ and ~~#1136714~~), but reward are the same $500?

Comment 29 by amyressler@google.com on Thu, Apr 1, 2021, 1:25 PM EDT

Hi, zyzengstorm@. The panel took your questions and concerns about potential for increased severity your Comment #6, Comment #7, and Comment #12 under consideration, as well as the developers' responses to them, when reward amount was decided. While Payments is important, we consider anywhere a bug that introduces potential user harm to be important, and bug reports are judged based on exploitability and impact of the issue presented, as well as the report quality itself.

The VRP Panel has the discretion to reward lower if a bug seems less exploitable and of lesser severity, and decided on $500 for this report.
All of this information in the report was taken into account by the VRP Panel and this amount was deemed appropriate for this bug report.

Comment 30 by zyzen...@gmail.com on Thu, Apr 1, 2021, 10:06 PM EDT

okay, I know.

Compared with the rewards of aosp, it is also the text injection that causes the meaning of the dialog box to change. The bonus of chrome is too low. I hope to chromium team can pay attention to this kind of UI logic vulnerabilities that are more intuitive to users.

Comment 31 by amyressler@google.com on Fri, Apr 2, 2021, 11:56 AM EDT
**Labels:** -reward-unpaid reward-inprocess

Comment 32 by zyzen...@gmail.com on Sat, Apr 24, 2021, 9:57 PM EDT

Hi @amyressler, please credit to @retsew0x01, thanks very much.

----------
My employer does not want us to report vulnerabilities, so I need to modify the id to achieve anonymity

Comment 33 by amyressler@chromium.org on Mon, Apr 26, 2021, 11:00 AM EDT

Hi zyzengstorm, updated in our system and all forthcoming and future release notes will credit your findings to @retsew0x01 :)

Comment 34 by amyressler@chromium.org on Mon, May 24, 2021, 11:20 AM EDT

**Labels:** Release-0-M91

Comment 35 by amyressler@google.com on Mon, May 24, 2021, 2:19 PM EDT

**Labels:** CVE-2021-30540 CVE_description-missing

Comment 36 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT

**Labels:** -CVE_description-missing CVE_description-submitted

Comment 37 by sheriffbot on Thu, Jun 24, 2021, 1:53 PM EDT

**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

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy