Starred by 2 users

Owner:	tsepez@chromium.org
CC:	thestig@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Plugins>PDF
Modified:	Jun 28, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Mac
Pri:	2
Type:	Bug-Security

reward-500
Security_Severity-Low
Security_Impact-Stable
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
Release-0-M89
external_security_report
CVE-2021-21190
external_security_bug

Issue 1166091: Security: Use of conditionally uninitialised stack variable may leak stack state

Reported by zhoua...@gmail.com on Wed, Jan 13, 2021, 2:42 AM EST

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36

Steps to reproduce the problem:
1.
2.
3.

What is the expected behavior?

What went wrong?
.

Did this work before? N/A

Chrome version: 87.0.4280.141 Channel: stable
OS Version: OS X 10.15.7
Flash Version:

Comment 1 Deleted

Comment 2 by sheriffbot on Wed, Jan 13, 2021, 2:46 AM EST

Labels: reward-potential

Comment 3 Deleted

Comment 4 by xinghuilu@chromium.org on Wed, Jan 13, 2021, 2:56 PM EST

Status: Assigned (was: Unconfirmed)
Owner: tsepez@chromium.org
Cc: thestig@chromium.org
Labels: Security_Severity-High Security_Impact-None
Components: Internals>Plugins>PDF

Thanks for the report. I think DCHECKs are in place to make sure stack variables are initialized. Tentatively set severity to high. +tsepez, could you take a look? Thanks!

Comment 5 by tsepez@chromium.org on Wed, Jan 13, 2021, 4:27 PM EST

Status: Started (was: Assigned)

Agreed. DCHECKS() are generally useless. Will put together a simple patch.

Comment 6 by tsepez@chromium.org on Wed, Jan 13, 2021, 4:30 PM EST

Labels: -Security_Severity-High Security_Severity-Low

Marking sev-low because there would need to show a way to trigger this path from actual content.

Comment 7 by bugdroid on Wed, Jan 13, 2021, 6:56 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/2355c635ab7c530c0191c12d4e191861055d696b

commit 2355c635ab7c530c0191c12d4e191861055d696b
Author: Tom Sepez <tsepez@chromium.org>
Date: Wed Jan 13 23:56:00 2021

Validate return code from FPDF_PageToDevice()

A DCHECK() here isn't sufficient to prevent the use of uninitialized
memory should this someday return false.

~~Bug: 1166084~~
Change-Id: I4cfd28653f2e6882f227299d68605be706b75b44
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2628044
Reviewed-by: K. Moon <kmoon@chromium.org>
Commit-Queue: Tom Sepez <tsepez@chromium.org>
Cr-Commit-Position: refs/heads/master@{#843247}

[modify] https://crrev.com/2355c635ab7c530c0191c12d4e191861055d696b/pdf/pdfium/pdfium_page.cc

Comment 8 Deleted

Comment 9 by xinghuilu@chromium.org on Thu, Jan 14, 2021, 2:23 PM EST

Labels: -Security_Impact-None Security_Impact-Stable

You're right, I think it should be Security_Impact-Stable.

Comment 10 by tsepez@chromium.org on Thu, Jan 14, 2021, 5:39 PM EST

Status: Fixed (was: Started)

Comment 11 by sheriffbot on Fri, Jan 15, 2021, 1:57 PM EST

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

Comment 12 by adetaylor@google.com on Wed, Jan 20, 2021, 6:58 PM EST

Labels: -reward-potential external_security_report

Comment 13 by sheriffbot on Thu, Jan 21, 2021, 12:43 PM EST

Labels: reward-topanel

Comment 14 Deleted

Comment 15 Deleted

Comment 16 by amyressler@google.com on Fri, Feb 26, 2021, 11:21 AM EST

Hello, zhouat2017@. Our apologies for the delay on an outcome on this. Since this issue is of low security severity, it has not yet come up in the VRP Panel for decision on reward eligibility. Priority and decision are based on exploitability and security impact so it's taking a little extra time on this one.

There will be an update on this issue when a VRP panel decision has been made on this issue, so no effort is required on your part to check in. Thank you for your patience!

Comment 17 by amyressler@google.com on Fri, Feb 26, 2021, 12:36 PM EST

I am realizing that I didn't address your CVE question in my four responses, so I wanted to update you about that. CVE assignment occurs when the fix for that bug is released. That will also be updated on each issue, so you will get an update when that occurs. Thank you.

Comment 18 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST

Labels: Release-0-M89

Comment 19 by adetaylor@google.com on Mon, Mar 1, 2021, 7:29 PM EST

Labels: CVE-2021-21190 CVE_description-missing

Comment 20 by amyressler@google.com on Tue, Mar 9, 2021, 12:59 PM EST

Labels: -CVE_description-missing CVE_description-submitted

Comment 21 by sheriffbot on Wed, Mar 10, 2021, 8:04 PM EST

Labels: reward-potential

Comment 22 by zhangtiff@google.com on Wed, Mar 17, 2021, 7:13 PM EDT

Labels: -reward-potential external_security_bug

Comment 23 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 24 by amyressler@google.com on Wed, Mar 31, 2021, 7:12 PM EDT

Hello, zhouat2017@ - the VRP Panel has decided to reward you $500 for this report.

Comment 25 by amyressler@google.com on Fri, Apr 2, 2021, 12:03 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 26 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

Comment 27 by amyressler@chromium.org on Mon, Jun 28, 2021, 11:47 AM EDT

Hello zhouat- we consider attachments/pocs in comments as part of the reports to be an integral part of the report, so I've un-deleted them. Thanks!