☆ Starred by 1 user

Owner:	tsepez@chromium.org
CC:	thestig@chromium.org
Status:	Verified *(Closed)*
Components:	Internals>Plugins>PDF
Modified:	Jan 22, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
reward-7500
allpublic
reward-inprocess
ClusterFuzz-Verified
CVE_description-submitted
M-86
Target-86
FoundIn-83
FoundIn-84
merge-merged-4240
merge-merged-86
merge-merged-4280
merge-merged-87
Release-2-M86
CVE-2020-16002

Issue 1137630: Security: PDFium heap-use-after-free in CPWL_ListBox::~CPWL_ListBox()

Reported by merc....@gmail.com on Mon, Oct 12, 2020, 10:08 PM EDT

Code

UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/537.36

Steps to reproduce the problem:
1 build chrome with asan
2 ./chrome uaf0.pdf

If you want to get the symbol info, close the sandbox: ./chrome --no-sandbox uaf0.pdf

Note that this affect stable version.

What is the expected behavior?

What went wrong?
In function CPWL_ListBox::~CPWL_ListBox() at third_party/pdfium/fpdfsdk/pwl/cpwl_list_box.cpp:73
the `m_pList` will be deleted at 0x5555692518d5(asm), then at 0x555569251903(asm), the program will call the destructor of CPWL_ListCtrl

```
   0x5555692518d5 <~CPWL_ListBox()+245>:     call   0x55555f1a8930 <operator delete()>
   0x5555692518da <~CPWL_ListBox()+250>:     lea    rdi,[r14+0x140]
   0x5555692518e1 <~CPWL_ListBox()+257>:     mov    rax,rdi
   0x5555692518e4 <~CPWL_ListBox()+260>:     shr    rax,0x3
   0x5555692518e8 <~CPWL_ListBox()+264>:     cmp    BYTE PTR [rax+0x7fff8000],0x0
   0x5555692518ef <~CPWL_ListBox()+271>:     jne    0x55556925196b <~CPWL_ListBox()+395>
   0x5555692518f1 <~CPWL_ListBox()+273>:     mov    rbx,QWORD PTR [rdi]
   0x5555692518f4 <~CPWL_ListBox()+276>:     mov    QWORD PTR [rdi],0x0
   0x5555692518fb <~CPWL_ListBox()+283>:     test   rbx,rbx
   0x5555692518fe <~CPWL_ListBox()+286>:     je     0x555569251910 <~CPWL_ListBox()+304>
   0x555569251900 <~CPWL_ListBox()+288>:     mov    rdi,rbx
   0x555569251903 <~CPWL_ListBox()+291>:     call   0x555569254870 <~CPWL_ListCtrl()>
```

The destructor will call Clear => InvalidateItem(-1) => IOnInvalidateRect => m_pList is used again => UAF occurs.

In third_party/pdfium/fpdfsdk/pwl/cpwl_list_impl.cpp:101

```
100 CPWL_ListCtrl::~CPWL_ListCtrl() {
101   Clear();
102 }
```

third_party/pdfium/fpdfsdk/pwl/cpwl_list_impl.cpp:520

```
518 void CPWL_ListCtrl::Clear() {
519   m_ListItems.clear();
520   InvalidateItem(-1);
521 }
```

third_party/pdfium/fpdfsdk/pwl/cpwl_list_impl.cpp:358

```
352 void CPWL_ListCtrl::InvalidateItem(int32_t nItemIndex) {
```

```
353   if (m_pNotify) {
354     if (nItemIndex == -1) {
355       if (!m_bNotifyFlag) {
356         m_bNotifyFlag = true;
357         CFX_FloatRect rcRefresh = m_rcPlate;
358         m_pNotify->IOnInvalidateRect(&rcRefresh);
359         m_bNotifyFlag = false;
360       }
```

third_party/pdfium/fpdfsdk/pwl/cpwl_list_box.cpp:64

```
 63 void CPWL_List_Notify::IOnInvalidateRect(CFX_FloatRect* pRect) {
 64   m_pList->InvalidateRect(pRect);
 65 }
```

find the attached poc and asan log

Did this work before? N/A

Chrome version: 86.0.4240.75 Channel: stable
OS Version: ubuntu20
Flash Version:

uaf0.pdf
4.1 KB Download

asan.txt
25.8 KB View Download

Comment 1 by palmer@chromium.org on Tue, Oct 13, 2020, 1:29 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: tsepez@chromium.org
Cc: thestig@chromium.org
Labels: Security_Severity-High Security_Impact-Stable OS-Chrome OS-Fuchsia OS-Mac OS-Windows Pri-1
Components: Internals>Plugins>PDF

Thanks for this report! tsepez, passing to you.

Comment 2 by tsepez@chromium.org on Tue, Oct 13, 2020, 2:10 PM EDT Project Member

Labels: -Via-Wizard-Security

I'm not immediately reproducing on ToT though your asan trace clearly indicates a problem. Is there some interaction required - keystrokes, mouse, etc?
Leaving severity high for the moment, though I think it might be hard to get much control between the use and the free. My speculation is that inverting the order of the following in cpwl_list_box.h may close the window by destroying the listctrl first:

```
  std::unique_ptr<CPWL_ListCtrl> m_pList;
  std::unique_ptr<CPWL_List_Notify> m_pListNotify;
```

but I can't confirm this without getting the repro myself.

Comment 3 by merc....@gmail.com on Tue, Oct 13, 2020, 2:23 PM EDT

I test is on Mac, it can still crash the PDF process, while windows not...

Comment 4 by thestig@chromium.org on Tue, Oct 13, 2020, 2:26 PM EDT Project Member

I'll try to repro later today if needed.

Comment 5 by merc....@gmail.com on Tue, Oct 13, 2020, 2:29 PM EDT

And still repo on latest stable version on Ubuntu:)

Comment 6 by thestig@chromium.org on Tue, Oct 13, 2020, 4:07 PM EDT Project Member

tsepez: Repros out of the box for me.

Comment 7 by tsepez@chromium.org on Tue, Oct 13, 2020, 4:52 PM EDT Project Member

Resync'd to 4dd6f4ab, now getting crash in Asan + Debug, but I have to drag the scrollbar up and down. Debug assert hit:

```
  cpwl_wnd.cpp:122: virtual CPWL_Wnd::~CPWL_Wnd(): Assertion `!m_bCreated' failed.
```

I'll try rebuilding with Asan - debug.

Comment 8 by thestig@chromium.org on Tue, Oct 13, 2020, 4:57 PM EDT Project Member

tsepez: I repro'd with this set of GN args:

```
dcheck_always_on = true
is_debug = false
is_asan = true
is_component_build = false
is_lsan = true
symbol_level = 1
```

Given it happens out of the box for me, maybe we can feed the input into ClusterFuzz and let it process the input.

Comment 9 by tsepez@chromium.org on Tue, Oct 13, 2020, 5:13 PM EDT Project Member

Ok, I nuked my directory and will try again. In the mean time, If you invert the two lines as in comment two, is it resolved?

Comment 10 by thestig@chromium.org on Tue, Oct 13, 2020, 5:24 PM EDT Project Member

I uploaded the test case to CF: https://clusterfuzz.com/testcase-detail/5649023791071232

Comment 11 by ClusterFuzz on Tue, Oct 13, 2020, 5:30 PM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5750442330226688.

Comment 12 by thestig@chromium.org on Tue, Oct 13, 2020, 5:33 PM EDT Project Member

Whoops, we started 2 CF jobs. I'll mark mine as a duplicate when it finishes.

Comment 13 by tsepez@chromium.org on Tue, Oct 13, 2020, 6:18 PM EDT Project Member

CF seems to have repro'd it at https://clusterfuzz.com/testcase-detail/5750442330226688

Comment 14 by ClusterFuzz on Wed, Oct 14, 2020, 1:00 PM EDT Project Member

Labels: FoundIn-84 FoundIn-83

Detailed Report: https://clusterfuzz.com/testcase?key=5750442330226688

Fuzzer:

Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Heap-use-after-free READ 8
Crash Address: 0x60900004fa00
Crash State:
  CPWL_List_Notify::IOnInvalidateRect
  CPWL_ListCtrl::Clear
  CPWL_ListCtrl::~CPWL_ListCtrl

Sanitizer: address (ASAN)

Recommended Security Severity: High

Crash Revision: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&revision=816706

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5750442330226688

The reproduce tool requires a ClusterFuzz source checkout. To prepare one, run:

```
git clone https://github.com/google/clusterfuzz && cd clusterfuzz && git checkout tags/reproduce-tool-stable
```

To reproduce this issue, run:

```
./reproduce.sh -t https://clusterfuzz.com/testcase-detail/5750442330226688 -b /path/to/build
```

Please use the GN arguments provided in this report when building the binary. If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 15 by bugdroid on Wed, Oct 14, 2020, 1:23 PM EDT Project Member

The following revision refers to this bug:
  https://pdfium.googlesource.com/pdfium/+/7dd9dbd6dd4959a568e7701da19871f859f8dce2

commit 7dd9dbd6dd4959a568e7701da19871f859f8dce2
Author: Tom Sepez <tsepez@chromium.org>
Date: Wed Oct 14 17:20:54 2020

Reverse order of CPWL_ListCtrl and CPWL_List_Notify cleanup

(Speculative) fix for the crash in 1137630, since it only reproduces
sporadically on my system, but hasn't re-occured since applying the
patch.

~~Bug: chromium:1137630~~
Change-Id: I4f52c7109eca00dfa8faee9bc6341cd94c25b60c
Reviewed-on: https://pdfium-review.googlesource.com/c/pdfium/+/75090
Reviewed-by: Lei Zhang <thestig@chromium.org>
Commit-Queue: Tom Sepez <tsepez@chromium.org>

[modify] https://pdfium.googlesource.com/pdfium/+/7dd9dbd6dd4959a568e7701da19871f859f8dce2/fpdfsdk/pwl/cpwl_list_box.h

Comment 16 by sheriffbot on Wed, Oct 14, 2020, 1:57 PM EDT Project Member

Labels: M-86 Target-86

Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 17 by bugdroid on Thu, Oct 15, 2020, 2:46 AM EDT Project Member

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src.git/+/7f50adf717f86137b7ec43b6ddcb9aa81bc28941

commit 7f50adf717f86137b7ec43b6ddcb9aa81bc28941
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Thu Oct 15 06:44:17 2020

Roll PDFium from a58a676ab96a to 055495dfbb24 (3 revisions)

https://pdfium.googlesource.com/pdfium.git/+log/a58a676ab96a..055495dfbb24

2020-10-15 tsepez@chromium.org Split IPWL_FillerNotify off into its own .h file.
2020-10-14 tsepez@chromium.org Replace class CFWL_List_Notify with a virtual interface.
2020-10-14 tsepez@chromium.org Reverse order of CPWL_ListCtrl and CPWL_List_Notify cleanup

If this roll has caused a breakage, revert this CL and stop the roller
using the controls here:
https://autoroll.skia.org/r/pdfium-autoroll
Please CC pdfium-deps-rolls@chromium.org on the revert to ensure that a human
is aware of the problem.

To report a problem with the AutoRoller itself, please file a bug:
https://bugs.chromium.org/p/skia/issues/entry?template=Autoroller+Bug

Documentation for the AutoRoller is here:
https://skia.googlesource.com/buildbot/+doc/master/autoroll/README.md

~~Bug: chromium:1137630~~
Tbr: pdfium-deps-rolls@chromium.org
Change-Id: I6e712a2220f4569d1a354a44064a434d35253e2f
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2473826
Reviewed-by: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Commit-Queue: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Cr-Commit-Position: refs/heads/master@{#817397}

[modify] https://crrev.com/7f50adf717f86137b7ec43b6ddcb9aa81bc28941/DEPS

Comment 18 by ClusterFuzz on Thu, Oct 15, 2020, 4:06 PM EDT Project Member

Status: Verified (was: Assigned)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5750442330226688 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=817395:817399

If this is incorrect, please add the ClusterFuzz-Wrong label and re-open the issue.

Comment 19 by sheriffbot on Fri, Oct 16, 2020, 3:08 PM EDT Project Member

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

Comment 20 by sheriffbot on Fri, Oct 16, 2020, 3:28 PM EDT Project Member

Labels: Merge-Request-87 Merge-Request-86

Requesting merge to stable M86 because latest trunk commit (817397) appears to be after stable branch point (800218).

Requesting merge to beta M87 because latest trunk commit (817397) appears to be after beta branch point (812852).

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

Comment 21 by sheriffbot on Fri, Oct 16, 2020, 3:33 PM EDT Project Member

Labels: -Merge-Request-87 Merge-Review-87 Hotlist-Merge-Review

This bug requires manual review: DEPS changes referenced in bugdroid comments.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- 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?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna @(iOS), cindyb@(ChromeOS), lakpamarthy@(Desktop)

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

Comment 22 by lakpamarthy@google.com on Fri, Oct 16, 2020, 7:20 PM EDT Project Member

tsepez@ - please address the merge questionnaire in c#21 to consider the approval? Thanks!

Comment 23 by adetaylor@google.com on Sun, Oct 18, 2020, 4:52 PM EDT Project Member

Labels: reward-topanel

Comment 24 by adetaylor@chromium.org on Mon, Oct 19, 2020, 10:31 AM EDT Project Member

Labels: -Merge-Request-86 -Merge-Review-87 Merge-Approved-86 Merge-Approved-87

Even in the absence of the questions, approving merge to M86 (branch 4240) and M87 (branch 4280) because the fix looks very simple.

Comment 25 by tsepez@chromium.org on Mon, Oct 19, 2020, 12:24 PM EDT Project Member

Merges created at
https://pdfium-review.googlesource.com/c/pdfium/+/75351 [M87]
https://pdfium-review.googlesource.com/c/pdfium/+/75350 [M86]

But getting red skia bots. We've not merge to these branches in a while. Might be pre-existing, and we don't ship skia, but this is delayed until I resolve the bots.

ade - I wouldn't let this block the release as there is a small window between the two frees which makes exploitation less likely.

Comment 26 by bugdroid on Mon, Oct 19, 2020, 1:06 PM EDT Project Member

Labels: -merge-approved-87 merge-merged-87 merge-merged-4280

The following revision refers to this bug:
https://pdfium.googlesource.com/pdfium/+/0950ad89ea1123b71be05b3c5c4223c2934a976f

commit 0950ad89ea1123b71be05b3c5c4223c2934a976f
Author: Tom Sepez <tsepez@chromium.org>
Date: Mon Oct 19 17:06:10 2020

[M87] Reverse order of CPWL_ListCtrl and CPWL_List_Notify cleanup

(Speculative) fix for the crash in 1137630, since it only reproduces
sporadically on my system, but hasn't re-occured since applying the
patch.

TBR: thestig@chromium.org
~~Bug: chromium:1137630~~
Change-Id: I4f52c7109eca00dfa8faee9bc6341cd94c25b60c
Reviewed-on: https://pdfium-review.googlesource.com/c/pdfium/+/75090
Reviewed-by: Lei Zhang <thestig@chromium.org>
Commit-Queue: Tom Sepez <tsepez@chromium.org>
(cherry picked from commit 7dd9dbd6dd4959a568e7701da19871f859f8dce2)
Reviewed-on: https://pdfium-review.googlesource.com/c/pdfium/+/75351
Reviewed-by: Tom Sepez <tsepez@chromium.org>

[modify] https://pdfium.googlesource.com/pdfium/+/0950ad89ea1123b71be05b3c5c4223c2934a976f/fpdfsdk/pwl/cpwl_list_box.h

Comment 27 by tsepez@chromium.org on Mon, Oct 19, 2020, 1:09 PM EDT Project Member

Red bots pre-existing and we don't ship skia. Landing both patches.

Comment 28 by bugdroid on Mon, Oct 19, 2020, 1:10 PM EDT Project Member

Labels: -merge-approved-86 merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://pdfium.googlesource.com/pdfium/+/9591642a0896c0bd7377ce1eadf782eccc0e0b9b

commit 9591642a0896c0bd7377ce1eadf782eccc0e0b9b
Author: Tom Sepez <tsepez@chromium.org>
Date: Mon Oct 19 17:07:57 2020

[M86] Reverse order of CPWL_ListCtrl and CPWL_List_Notify cleanup

(Speculative) fix for the crash in 1137630, since it only reproduces
sporadically on my system, but hasn't re-occured since applying the

patch.

TBR: thestig@chromium.org
~~Bug: chromium:1137630~~
Change-Id: I4f52c7109eca00dfa8faee9bc6341cd94c25b60c
Reviewed-on: https://pdfium-review.googlesource.com/c/pdfium/+/75090
Reviewed-by: Lei Zhang <thestig@chromium.org>
Commit-Queue: Tom Sepez <tsepez@chromium.org>
(cherry picked from commit 7dd9dbd6dd4959a568e7701da19871f859f8dce2)
Reviewed-on: https://pdfium-review.googlesource.com/c/pdfium/+/75350
Reviewed-by: Tom Sepez <tsepez@chromium.org>

[modify] https://pdfium.googlesource.com/pdfium/+/9591642a0896c0bd7377ce1eadf782eccc0e0b9b/fpdfsdk/pwl/cpwl_list_box.h

Comment 29 by adetaylor@google.com on Mon, Oct 19, 2020, 11:09 PM EDT Project Member

Labels: Release-2-M86

Comment 30 by adetaylor@google.com on Wed, Oct 21, 2020, 7:12 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-7500

*** 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 31 by adetaylor@google.com on Wed, Oct 21, 2020, 7:20 PM EDT Project Member

Congratulations, the VRP panel has decided to award $7,500 for this bug.

Comment 32 by adetaylor@google.com on Thu, Oct 22, 2020, 12:25 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 33 by awhalley@google.com on Fri, Oct 23, 2020, 2:28 PM EDT Project Member

Undeleting attachments in comment 0 as they are considered part of the report.

Comment 34 by adetaylor@google.com on Sun, Dec 6, 2020, 12:59 AM EST Project Member

Labels: CVE-2020-16002 CVE_description-missing

Comment 35 by adetaylor@google.com on Thu, Jan 7, 2021, 2:03 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 36 by sheriffbot on Fri, Jan 22, 2021, 1:52 PM EST 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