

Closed Bug 1606619 (CVE-2020-6794) Opened 3 years ago Closed 3 years ago

key3.db encryption key remains on disk from Thunderbird 52.x (becomes issue if adding a master password post 60.x)

Categories

Product: Thunderbird
Component: Security
Version: 60

Type: defect
Priority: Not set Severity: normal

Tracking

Status: RESOLVED FIXED
Milestone: Thunderbird 74.0

Tracking Flags: thunderbird_esr68
Tracking Status: fixed

People

(Reporter: KaiE, Assigned: KaiE)

References

Details

(Keywords: sec-moderate)

Attachments

[testing-bug-1606619.txt](#)

3 years ago Kai Engert (KaiE)
2.51 KB, text/plain

[Details](#)

[1606619-complete-v3.patch](#)

3 years ago Kai Engert (KaiE)
5.54 KB, patch

[Details](#) | [Diff](#) | [Splinter Review](#)

Show Obsolete

Bottom

Tags

Timeline



Kai Engert (KaiE) Assignee
Description • 3 years ago



We haven't yet fixed [bug-1475775](#) in Thunderbird.

Because of the risk of key dataloss (e.g. [bug-1510212](#)), we're waiting for a solution that is more reliable than what Firefox had used as a fix.

Let's use this new bug to track fixing the issue in Thunderbird.

In separate NSS [bug-1561360](#) we're working out an appropriate solution, potentially at the NSS code level.



Kai Engert (KaiE) Assignee
Updated • 3 years ago



See Also: → [1561366](#)



Kai Engert (KaiE) Assignee
Updated • 3 years ago



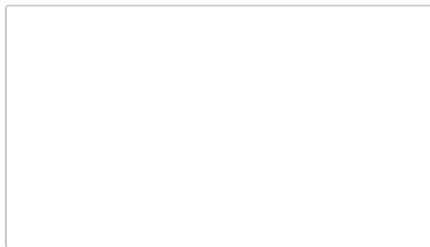
See Also: → [1510212](#)



Kai Engert (KaiE) Assignee
Comment 1 • 3 years ago



Attached file [testing-bug-1606619.txt](#) — [Details](#)



Assignee: nobody → kaie



Kai Engert (KaiE) Assignee
Updated • 3 years ago



Summary: Fix CVE-2018-12383 in Thunderbird → Fix CVE-2018-12383 in Thunderbird 68.x



Kai Engert (KaiE) Assignee
Comment 2 • 3 years ago



Attached patch [1606619-v1.patch \(intended for the fork of the Mozilla repository used by Thunderbird 68.x\)](#) (obsolete) — [Details](#) — [Splinter Review](#)



Kai Engert (KaiE) Assignee
Comment 3 • 3 years ago



The attached patch applies to TB 68.x, only.

The patch doesn't make sense for any later Thunderbird versions, because:

- we didn't take [bug-1561366](#) for comm-central, which means, thunderbird versions 69.x+ already deleted key3.db
- mozilla branch 73+ has disabled support for key3.db (dbm file format) completely ([bug-1594934](#)), which means, versions 73+ are no longer able to perform a migration from key3.db to key4.db

If my patch is wrong, it will cause dataloss for those users who will upgrade from thunderbird 52.x to a thunderbird 68.x having this fix.

However, with the testing steps listed in the attached text file, which I have executed locally, I try to show that the patch will delete key3.db only after the migration was successful.



Kai Engert (:KaiE:) Assignee
Updated • 3 years ago



Attachment #9119188 - Attachment description: 1606619-v1.patch → 1606619-v1.patch (intended for the fork of the Mozilla repository used by Thunderbird 68.x)



Masatoshi Kimura [:emk]
Comment 4 • 3 years ago



Comment on [attachment 9119188 \[details\] \[diff\] \[review\]](#)
1606619-v1.patch (intended for the fork of the Mozilla repository used by Thunderbird 68.x)

Review of [attachment 9119188 \[details\] \[diff\] \[review\]](#):

```
::: security/manager/ssl/SecretDecoderRing.cpp
@@ +200,5 @@
> + nsCOMPtr<nsIFile> file = do_CreateInstance("@mozilla.org/file/local;1");
> + if (!file) {
> +     return NS_ERROR_FAILURE;
> + }
> + nsresult rv = file->InitWithNativePath(path);
```

See [bug-1607652](#).



Kai Engert (:KaiE:) Assignee
Updated • 3 years ago



See Also: → [1607652](#)



Kai Engert (:KaiE:) Assignee
Comment 5 • 3 years ago



Bob, thanks again for your very helpful comments in [bug-1561368](#).

Bob, can I assume, if we aren't merging,

```
slot = PK11_GetInternalKeySlot()
bool done = !PK11_IsReadOnly(slot) && PK11_IsLoggedIn(slot, NULL);
```

and `done` is true, that the migration from key3.db to key4.db has already completed?

FYI, the attached patch implements the following strategy:

- don't remove key3.db by default (as Firefox does it)
- wait until we've successfully decrypted a string stored in the secret decoder. If that works, either no master password is configured, or the master password was correctly provided by the user.
- at this time, do a once-per-application-session check for the potential cleanup
- double-check that our internal token is really logged in (we assume this means the data was migrated), and that we aren't in read-only mode (this ensures that a migration to key4.db was allowed to be written to disk)
- confirm that key4.db exists on disk. If it doesn't exist, stop.
- check whether key3.db exists on disk. If it exists, delete it.

Flags: needinfo?(rrelyea)



Robert Relyea
Comment 6 • 3 years ago



That should work. The only possible issue is if the update failed after the login in a way that it will try to update again. I don't see a good way of detecting this case.

Flags: needinfo?(rrelyea)



Kai Engert (:KaiE:) Assignee
Comment 7 • 3 years ago



Comment on [attachment 9119188 \[details\] \[diff\] \[review\]](#)
1606619-v1.patch (intended for the fork of the Mozilla repository used by Thunderbird 68.x)

Magnus, given Bob approved the strategy, are you OK to take this fix for stable Thunderbird 68.x (only)?

Any suggestion who might want to double-check my fix, by potentially playing with the separate test instructions I've attached?

Attachment #9119188 - Flags: review?(mkmelin+mozilla)



Kai Engert (:KaiE:) Assignee
Comment 8 • 3 years ago













regarding [comment 4](#), I'd merge that fix into this patch once that one is reviewed

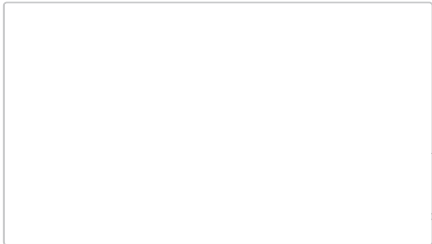


Magnus Melin [:mkmelin]
Comment 9 • 3 years ago



Comment on [attachment 9119188 \[details\] \[diff\] \[review\]](#)
1606619-v1.patch (intended for the fork of the Mozilla repository used by Thunderbird 68.x)

Review of attachment-9119188 [details] [diff] [review]: -----		
Seems fine to me.		
Maybe you can let Khushil go through the steps an see if he can verify.		
Attachment #9119188 - Flags: review?(mkmelin+mozilla) → review+		
	Magnus Melin [:mkmelin] Updated • 3 years ago	<div>—</div>
Status: NEW → ASSIGNED		
	Masatoshi Kimura [:emk] Comment 10 • 3 years ago	<div>—</div>
Please port bug-1607652 . Thunderbird 68 is the last chance to upgrade from DBM and clean-up key3.db correctly without dataloss.		
	Kai Engert (:KaiE:) Assignee Comment 11 • 3 years ago	<div>—</div>
Attached patch 1606619-1607652.patch (obsolete) — Details — Splinter Review		
emk, can you please review this incremental patch, to confirm it's correctly and completely merged for the key3.db scenario?		
Attachment #9120253 - Flags: review?(VYV03354)		
	Masatoshi Kimura [:emk] Comment 12 • 3 years ago	<div>—</div>
Comment on attachment-9120253 [details] [diff] [review] 1606619-1607652.patch		
Review of attachment-9120253 [details] [diff] [review]: -----		
LGTM		
Attachment #9120253 - Flags: review?(VYV03354) → review+		
	Kai Engert (:KaiE:) Assignee Comment 13 • 3 years ago	<div>—</div>
Attached patch 1606619-complete-v2.patch (obsolete) — Details — Splinter Review		
This patch combines the two earlier patches into a single patch, and adds a review comment.		
Attachment #9119188 - Attachment is obsolete: true		
Attachment #9120253 - Attachment is obsolete: true		
Attachment #9120287 - Flags: review+		
	Kai Engert (:KaiE:) Assignee Comment 14 • 3 years ago	<div>—</div>
(In reply to Magnus Melin [:mkmelin] from comment #9)		
Maybe you can let Khushil go through the steps an see if he can verify.		
Hi Khushil, may I ask for your help to test this change?		
I haven't been able to create a try build yet, so you'd have to build locally.		
Only for comm-esr68, and the patch is for mozilla-esr68 and THUNDERBIRD_68_VERBRANCH.		
Test instructions are attached, too.		
	Kai Engert (:KaiE:) Assignee Comment 15 • 3 years ago	<div>—</div>
Khushil, please see comment 14 .		
	Kai Engert (:KaiE:) Assignee Comment 16 • 3 years ago	<div>—</div>
Looks like the try server is down, so maybe I'll be able to create a test build a bit later.		
	Kai Engert (:KaiE:) Assignee Comment 17 • 3 years ago	<div>—</div>
They've fixed it.		
Try build running here: https://treeherder.mozilla.org/#/jobs?repo=try-comm-central&revision=49cdb3d083ba692b84af334edc21a86a38c3e42d		
	Kai Engert (:KaiE:) Assignee Comment 18 • 3 years ago	<div>—</div>
Attached patch 1606619-complete-v3.patch — Details — Splinter Review		



(In reply to Kai Engert (:KaiE:) from [comment #47](#))

Try build running here:
<https://treeherder.mozilla.org/#/jobs?repo=try-comm-central&revision=49cdb3d083ba692b84af334edc21a86a38c3e42d>

The above has builds for Linux and Mac.

Windows build had failed because of a missing include. This updated patch fixes it. Successful try build for Windows is here:
<https://treeherder.mozilla.org/#/jobs?repo=try-comm-central&revision=0264197e4bd32135e3eb454df21e70ccbe39a01d>

Attachment #9120287 - Attachment is obsolete: true



Kai Engert (:KaiE:) Assignee
Comment 19 • 3 years ago



Comment on [attachment 9120340](#) [details] [diff] [review]
1606619-complete-v3.patch

ESR Uplift Approval Request

- **If this is not a sec{high,crit} bug, please state case for ESR consideration:** ESR 68.x is the last chance to fix this CVE for Thunderbird. We'll be unable to cleanup key3.db in TB 78, because TB 78 will no longer be able to perform a data migration.
- **User impact if declined:** Users having upgraded from TB 52.x will still be exposed to the security issue, because unprotected key3.db will remain on disk.
- **Fix Landed on Version:** n/a
- **Risk to taking this patch:** Medium
- **Why is the change risky/not risky? (and alternatives if risky):** There's a small potential risk for dataloss (of saved passwords and private keys), for people who'll upgrade directly from TB 52.x to TB 68.x with this fix. Bob Relyea stated that in theory, the logic we use to conclude that "migration to key4.db has completed" might produce a false positive in an edge case scenario, but he isn't aware of a way to test for that edge case.
Not at risk are people who have already used TB 60.x or previous TB 68.x for a while, and have already entered their master password several times. Those should certainly have been migrated successfully already.
- **String or UUID changes made by this patch:** none

Attachment #9120340 - Flags: approval-mozilla-esr68?



Jorg K (CEST = GMT+2)
Comment 20 • 3 years ago



Umm, is this a request for mozilla-esr68 trunk or THUNDERBIRD_68_VERBRANCH? For the latter, we don't ask for approval, we just land it there ;-)



Kai Engert (:KaiE:) Assignee
Comment 21 • 3 years ago



Comment on [attachment 9120340](#) [details] [diff] [review]
1606619-complete-v3.patch

Yeah, sorry, approval request for THUNDERBIRD_68_VERBRANCH.
Jörg, those comments were intended for you, to clarify and document the risks.

Before landing, we should wait for a positive test feedback from either Khushil or emk.

Attachment #9120340 - Flags: ~~approval-mozilla-esr68~~



Khushil Mistry (:khushil324)
Comment 22 • 3 years ago



Yes, it worked. I followed all the steps and finally, key3.db was not there in the profile.



Kai Engert (:KaiE:) Assignee
Comment 23 • 3 years ago



Khushil, thanks for testing.



Kai Engert (:KaiE:) Assignee
Comment 24 • 3 years ago



Hello Aryx, could you please commit [attachment 9120340](#) [details] [diff] [review] on mozilla-esr68/THUNDERBIRD_68_VERBRANCH ?
Thanks in advance














Magnus Melin (:mkmelin)
Comment 25 • 3 years ago



Aryx, see [comment 24](#).

Flags: needinfo?(aryx.bugmail)

 Kai Engert (:KaiE:) Assignee Updated • 3 years ago	—
status-thunderbird_esr68 : --- → affected tracking-thunderbird_esr68 : --- → ?	
 Kai Engert (:KaiE:) Assignee Updated • 3 years ago	—
Keywords: sec-moderate	
 Kai Engert (:KaiE:) Assignee Comment 26 • 3 years ago	—
Updating summary to match description from original Firefox bug-1475775 (CVE-2018-12383).	
Summary: Fix CVE-2018-12383 in Thunderbird 68.x → key3.db encryption key remains on disk from Thunderbird 52.x (becomes issue if adding a master password post 60.x)	
 Kai Engert (:KaiE:) Assignee Comment 27 • 3 years ago • Edited	—
[deleted, double post]	
 Kai Engert (:KaiE:) Assignee Comment 28 • 3 years ago	—
Hello Red Hat / CentOS people, cc'ing you FYI. If you have older RHEL branches that use patched NSS/FF/TB that is hardcoded to use key3.db/DBM, and which also gets Thunderbird 68.x updates, then you probably want to verify this patch is safe for you.	
 Tom Ritter [:tjr] Updated • 3 years ago	—
Alias: CVE-2020-6794	
 Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or bailout) Comment 29 • 3 years ago	—
https://hg.mozilla.org/releases/mozilla-esr68/rev/661669a9175b755a43bde8a1a6594cd93f3f75df Shall this only land on mozilla-central?	
Status: ASSIGNED → RESOLVED Closed: 3 years ago status-thunderbird_esr68 : affected → fixed Flags: needinfo2(aryx,bugmail) Resolution: --- → FIXED Target Milestone: --- → Thunderbird 68.0	
 Kai Engert (:KaiE:) Assignee Comment 30 • 3 years ago	—
Shall this only land on mozilla-central? No. Only for Thunderbird 68. Firefox already fixed this differently in bug-1475775 .	
 Kai Engert (:KaiE:) Assignee Comment 31 • 3 years ago	—
We'll attribute Jurgen as the original reporter of this Thunderbird issue, because it's the same as the Firefox issue reported in bug-1475775 .	
 Kai Engert (:KaiE:) Assignee Updated • 3 years ago	—
tracking-thunderbird_esr68 : ? → +	
 Magnus Melin [:mkmelin] Updated • 3 years ago	—
Target Milestone: Thunderbird 68.0 → Thunderbird 74.0	

You need to [log in](#) before you can comment on or make changes to this bug.

Top ↑