Copy Summary ▾ View ▾

Closed Bug 1710290 (CVE-2021-29956) Opened 2 years ago Closed 2 years ago

For OpenPGP secret keys imported with Thunderbird versions 78.8.1 - 78.10.1, the master password isn't effective

▾ **Categories**

Product:	MailNews Core ▾	Type:	defect
Component:	Security: OpenPGP ▾	Priority:	*Not set* Severity: --
Version:	79		

▾ **Tracking**

Status:	RESOLVED FIXED	Tracking Flags:	
Milestone:	90 Branch		

	Tracking	Status
thunderbird_esr78	+	fixed
thunderbird89	---	fixed

▸ **People** (Reporter: KaiE, Assigned: KaiE)

▸ **References** (Regression)

▸ **Details**

▾ **Attachments**

hotfix-js-1710290-v2.txt Details
2 years ago **Kai Engert (:KaiE:)**
1.21 KB, text/plain

Bug 1710290 - Part 1, preparations: Moving code and APIs, log number of unprotected keys, update a test key. r=mkmelin
2 years ago **Kai Engert (:KaiE:)**
48 bytes, text/x-phabricator-request
wsmwk : **approval-comm-beta+**
wsmwk : **approval-comm-esr78+**
Details | Review

Bug 1710290 - Part 2: Protect keys after import into permanent store, and add a test. r=mkmelin
2 years ago **Kai Engert (:KaiE:)**
48 bytes, text/x-phabricator-request
wsmwk : **approval-comm-beta+**
wsmwk : **approval-comm-esr78+**
Details | Review

Bug 1710290 - Part 3: Repairing, automatically protect any unprotected keys in storage. r=mkmelin
2 years ago **Kai Engert (:KaiE:)**
48 bytes, text/x-phabricator-request
wsmwk : **approval-comm-beta+**
wsmwk : **approval-comm-esr78+**
Details | Review

Show Obsolete

Bottom ↓ Tags ▾ Timeline ▾

Kai Engert (:KaiE:) Assignee
Description • 2 years ago

The default behavior of Thunderbird 78 is to use an automatic protection mechanism for OpenPGP secret keys. To protect the keys at rest, users are required to set a master password.

Versions from 78.8.1 until 78.10.1 contain a regression bug (introduced by ~~bug 1673239~~) that imports keys without protection. As a result, even having a master password set doesn't protect the local storage of the secret key.

I'm initially filing this as a security senstitive bug, however, I suggest to open this bug immediately (today), because several users have publicly reported on the Thunderbird e2ee mailing list that the master password protection is ineffective for them.

Kai Engert (:KaiE:) Assignee
Comment 1 • 2 years ago

The fix for this bug should:

- fix the import mechanism, to ensure all imported secret keys are immediately protected
- introduce an automatic repair mechanism, which scans for unprotected keys, and automatically enables protection for those keys

We should carefully prepare the fix, which may take a few days to create, review, test and release.

In the meantime, as a hotfix, it might be possible to offer advanced users a hotfix, which they can execute using the JavaScript/Error console.

Kai Engert (:KaiE:) Assignee
Comment 2 • 2 years ago • Edited

To check if you are affected by this bug, you may use the following procedure:

Step 1: Select and copy the following block of text:

```
function reportUnprotectedKeys() {
  const { RNP } = ChromeUtils.import(
    "chrome://openpgp/content/modules/RNP.jsm"
  );
  let [prot, unprot] = RNP.getProtectedKeysCount();
  console.log("Number of protected keys: " + prot);
  console.log("Number of unprotected keys: " + unprot);
}
reportUnprotectedKeys();
```

Step 2: Use the menu to open the error console. Either use the menu shown on the top of the Thunderbird window, or click the "burger menu" (three horizontal lines) in the upper right of the Thunderbird Window. Select Tools, Developer Tools, Error Console.

Step 3:
Click the space after the two blue arrows. Paste the block that you have selected above, then press the enter key.

The console will show a message saying "Number of unprotected keys". If the number shown is zero (0), you are not affected.

If a number other than zero is shown, you are affected by this bug.

Edit, 2021-05-11: Improved logging code as suggested in ~~comment 5~~ and ~~comment 6~~.

Wayne Mery (:wsmwk)
Comment 3 • 2 years ago

−

FYI we plan to do a 78.10.2 this week - but didn't plan to do another beta until next week.

Would we want to ship on both channels at same time? Or do we want it on beta first for a few days? The later would imply that we won't ship the patch on release channel until roughly next week.

Kai Engert (:KaiE:) Assignee
Comment 4 • 2 years ago • Edited

−

*Attached file ~~**hotfix-js-1710290-v1.txt**~~ (obsolete) — Details*

As a possible hotfix for advanced users, I am attaching a file with commands for repairing, that very likely should be safe for everyone to execute, whether affected or not affected by this bug. Let's test and review the hotfix.

Intended to be executed by affected users on the JS error console, if they don't want to wait for a fixed release.

Attachment #9220997 - Flags: review?(mkmelin+mozilla)

Rob Lemley [:rjl]
Comment 5 • 2 years ago

−

I suggest outputting the number of initial and post repair protected keys as well. It was the first question that popped into my head after running the repair function.

Magnus Melin [:mkmelin]
Comment 6 • 2 years ago

−

Comment on ~~attachment 9220997 [details]~~
hotfix-js-1710290-v1.txt

I'd lint it for readability.
Also move p declaration down to where it's first used. Or well, you don't need it at all. Just do if(!OpenPGPMasterpass._ensureMasterPassword())
For running in the console, the try catch is not useful I think.

What's the "repeat this procedure" about? To verify it worked? Maybe write that out in the msg if so.

Attachment #9220997 - Flags: ~~review?(mkmelin+mozilla)~~

Magnus Melin [:mkmelin]
Updated • 2 years ago

−

Status: NEW → ASSIGNED
status-thunderbird89: --- → affected
status-thunderbird_esr78: --- → affected
tracking-thunderbird_esr78: --- → +
Target Milestone: --- → 90 Branch

Kai Engert (:KaiE:) Assignee
Comment 7 • 2 years ago

−

Thanks, I will update the diagnosis and hotfix repair commands.

To fix the primary bug in Thunderbird, the following change needs to be reverted (only lines 1.97 to 1.104, not the whole patch):
https://hg.mozilla.org/releases/comm-esr78/rev/0c8606e7f45d805bf12d8e67828c24a343b34f11#l1.88

That will ensure that importing keys in the future will again result in protected keys.

It was my mistake to remove those lines. I had assumed that the new calls to rnp_key_protect would be sufficient to protect the keys. I should have verified my assumption. (The protection got lost when exporting the keys from the temporary area, although it shouldn't have gotten lost.)

I still need to work on the automatic repair. That's a bit tricky. The important decision is: at what time should the automatic repair be made? This decision is important, because repairing requires that the user has successfully entered the master password. I'm evaluating options.

Kai Engert (:KaiE:) Assignee
Comment 8 • 2 years ago

−

While working on a new automated test, I discovered an additional angle of this bug:

If the imported secret is unprotected (can be imported without entering the password), then the current code apparently works. RNP reports the imported key as a protected key.

Only if the imported secret is protected with a password, then the current code fails, and the imported key is reported as unprotected.

Kai Engert (:KaiE:) Assignee
Comment 9 • 2 years ago

−

*Attached file **hotfix-js-1710290-v2.txt** — Details*

Updated hotfix code, as suggested in ~~comment 5~~ and ~~comment 6~~.

Attachment #9220997 - Attachment is obsolete: true
Attachment #9221233 - Flags: review?(mkmelin+mozilla)

Kai Engert (:KaiE:) Assignee
Comment 10 • 2 years ago

Note I have edited ~~comment 2~~ with improved diagnostic logging, as suggested in ~~comment 5~~ and ~~comment 6~~.

Kai Engert (:KaiE:) Assignee
Comment 11 • 2 years ago

Attached file ***Bug 1710290 - Part 1, preparations: Moving code and APIs, log number of unprotected keys, update a test key. r=mkmelin*** *— Details*

Kai Engert (:KaiE:) Assignee
Comment 12 • 2 years ago

Attached file ***Bug 1710290 - Part 2: Protect keys after import into permanent store, and add a test. r=mkmelin*** *— Details*

Depends on D114823

Kai Engert (:KaiE:) Assignee
Comment 13 • 2 years ago

Attached file ***Bug 1710290 - Part 3: Repairing, automatically protect any unprotected keys in storage. r=mkmelin*** *— Details*

Depends on D114824

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

Group: ~~mail-core-security~~

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

Attachment #9221233 - Flags: ~~review?(mkmelin+mozilla)~~

Kai Engert (:KaiE:) Assignee
Comment 14 • 2 years ago

An experimental test build is available from the links below.
If you'd like to test it, please backup your profile.

linux64: https://firefox-ci-tc.services.mozilla.com/api/queue/v1/task/bBK_v-TPRMeINEQxDR5DOw/runs/0/artifacts/public/build/target.tar.bz2
linux32: https://firefox-ci-tc.services.mozilla.com/api/queue/v1/task/OOOv6eRCSiqsuNcTYIrwAQ/runs/0/artifacts/public/build/target.tar.bz2
win64: https://firefox-ci-tc.services.mozilla.com/api/queue/v1/task/HJkBP0nFT-OBFonTikh_Sg/runs/0/artifacts/public/build/target.zip
win32: https://firefox-ci-tc.services.mozilla.com/api/queue/v1/task/OlEaYmE5TI6ZfCb8w7afnA/runs/0/artifacts/public/build/target.zip
macos: https://firefox-ci-tc.services.mozilla.com/api/queue/v1/task/Jo1uSQkISxaiU5_EgYkzAw/runs/0/artifacts/public/build/target.dmg

Kai Engert (:KaiE:) Assignee
Comment 15 • 2 years ago

To clarify, the experimental build mentioned in the previous comment is based on latest 78.x

Pulsebot
Comment 16 • 2 years ago

Pushed by kaie@kuix.de:
https://hg.mozilla.org/comm-central/rev/0ab383eab07b
Part 1, preparations: Moving code and APIs, log number of unprotected keys, update a test key. r=mkmelin
https://hg.mozilla.org/comm-central/rev/5c58842e025a
Part 2: Protect keys after import into permanent store, and add a test. r=mkmelin
https://hg.mozilla.org/comm-central/rev/d5de99115896
Part 3: Repairing, automatically protect any unprotected keys in storage. r=mkmelin

Status: ASSIGNED → RESOLVED
Closed: 2 years ago
Resolution: --- → FIXED

Kai Engert (:KaiE:) Assignee
Comment 17 • 2 years ago

Comment on attachment 9221284 [details]
~~Bug 1710290~~ - Part 1, preparations: Moving code and APIs, log number of unprotected keys, update a test key. r=mkmelin

[Approval Request Comment]
Regression caused by (bug #): 1673239
User impact if declined: Local storage of OpenPGP secret keys may be unprotected despite master password.
Testing completed (on c-c, etc.): new automated test for regression fix. No feedback yet for automatic repairing.
Risk to taking this patch (and alternatives if risky): low to medium. Mostly code moving, new logging, and restoring a previously removed code block (adjusted after the offline primary key feature). Automatic repair code uses existing functions and is straightforward.

Attachment #9221284 - Flags: approval-comm-beta?

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

Attachment #9221285 - Flags: approval-comm-beta?

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

Attachment #9221286 - Flags: approval-comm-beta?

Wayne Mery (:wsmwk)
Comment 18 • 2 years ago

Comment on attachment 9221284 [details]
~~Bug 1710290~~ - Part 1, preparations: Moving code and APIs, log number of unprotected keys, update a test key. r=mkmelin

[Triage Comment]
Approved for beta

Attachment #9221284 - Flags: approval-comm-beta? → approval-comm-beta+

Wayne Mery (:wsmwk)
Comment 19 • 2 years ago

Comment on attachment 9221286 [details]
~~Bug 1710290~~ - Part 3: Repairing, automatically protect any unprotected keys in storage. r=mkmelin

[Triage Comment]
Approved for beta

Attachment #9221286 - Flags: approval-comm-beta? → approval-comm-beta+

Wayne Mery (:wsmwk)
Comment 20 • 2 years ago

Comment on attachment 9221285 [details]
~~Bug 1710290~~ - Part 2: Protect keys after import into permanent store, and add a test. r=mkmelin

[Triage Comment]
Approved for beta

Attachment #9221285 - Flags: approval-comm-beta? → approval-comm-beta+

Pulsebot
Comment 21 • 2 years ago

```
Pushed by geoff@darktrojan.net:
https://hg.mozilla.org/comm-central/rev/04f57699828a
follow-up - linting fix. rs=linting
```

Kai Engert (:KaiE:) Assignee
Comment 22 • 2 years ago

https://hg.mozilla.org/releases/comm-beta/rev/08585e2d0c668251f00212ce81d082a32d480320
https://hg.mozilla.org/releases/comm-beta/rev/498ff73e90a3c81f2a89c9012196ab58b2d49f7a
https://hg.mozilla.org/releases/comm-beta/rev/be0ed093191adfa7c91515bca973714858bb8dca
89.0b4

I missed the lint fix. Rob, can you please push ~~comment 21~~ to beta when finalizing the beta? I want to avoid a separate push.

status-thunderbird89: affected → fixed

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

Flags: needinfo?(rob)

Tom Ritter [:tjr]
Updated • 2 years ago

Alias: CVE-2021-29956

Rob Lemley [:rjl]
Comment 23 • 2 years ago
bugherder uplift

Thunderbird 89.0b4:
https://hg.mozilla.org/releases/comm-beta/rev/019b920cd5e0

Rob Lemley [:rjl]
Updated • 2 years ago

Flags: ~~needinfo?(rob)~~

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

Attachment #9221284 - Flags: approval-comm-esr78?

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

Attachment #9221285 - Flags: approval-comm-esr78?

Kai Engert (:KaiE:) Assignee
Updated • 2 years ago

Attachment #9221286 - Flags: approval-comm-esr78?

Wayne Mery (:wsmwk)
Comment 24 • 2 years ago

Comment on attachment 9221286 [details]
~~Bug 1710290~~ - Part 3: Repairing, automatically protect any unprotected keys in storage. r=mkmelin

[Triage Comment]
Approved for esr78

Attachment #9221286 - Flags: approval-comm-esr78? → approval-comm-esr78+

Wayne Mery (:wsmwk)
Comment 25 • 2 years ago

Comment on attachment 9221284 [details]
~~Bug 1710290~~ - Part 1, preparations: Moving code and APIs, log number of unprotected keys, update a test key. r=mkmelin

[Triage Comment]
Approved for esr78

Attachment #9221284 - Flags: approval-comm-esr78? → approval-comm-esr78+

Wayne Mery (:wsmwk)
Comment 26 • 2 years ago

Comment on attachment 9221285 [details]
~~Bug 1710290~~ - Part 2: Protect keys after import into permanent store, and add a test. r=mkmelin

[Triage Comment]
Approved for esr78

Attachment #9221285 - Flags: approval-comm-esr78? → approval-comm-esr78+

Kai Engert (:KaiE:) Assignee
Comment 27 • 2 years ago

78.10.2
https://hg.mozilla.org/releases/comm-esr78/rev/36ed28f4ec88f8d747399b538d5afd3e73702c94
https://hg.mozilla.org/releases/comm-esr78/rev/248ac0ef78f64b0c6a57dad759a34977fb73d481
https://hg.mozilla.org/releases/comm-esr78/rev/6657aa43703aaa1de16003c4ab7e92a1cbc6dff8

status-thunderbird_esr78: affected → fixed

Kai Engert (:KaiE:) Assignee
Comment 28 • 2 years ago

The RNP advisory can be found here:
https://www.rnpgp.org/advisories/ri-2021-001/

Thomas D. (:thomas8)
Updated • 6 months ago

Summary: For OpenPGP secret keys imported with Thunderbird versions 78.8.1 - 78.10.1 the master password isn't effective → For OpenPGP secret keys imported with Thunderbird versions 78.8.1 - 78.10.1, the master password isn't effective

You need to log in before you can comment on or make changes to this bug.

Top ↑