Copy Summary | View

Closed Bug 1673239 (CVE-2021-29950) Opened 2 years ago Closed 2 years ago

RNP-01-012 WP1 Thunderbird: Logic issue potentially leaves key material unlocked (Medium)

Categories

Product: MailNews Core
Component: Security: OpenPGP
Version: 78

Type: defect
Priority: Not set Severity: --

Tracking

Status: RESOLVED FIXED
Milestone: 87 Branch

Tracking Flags:	Tracking	Status
thunderbird_esr78	+	fixed

People (Reporter: wsmwk, Assigned: KaiE)

References

Details (Keywords: sec-moderate)

Attachments

Bug 1673239 - OpenPGP key material should remain locked in memory in failure scenarios. r=mkmelin
2 years ago **Kai Engert (:KaiE:)**
48 bytes, text/x-phabricator-request
wsmwk : **approval-comm-esr78+** Details | Review

Bottom ↓ | Tags | Timeline

Wayne Mery (:wsmwk) Reporter
Description • 2 years ago

During the audit of the RNP source code, it was discovered that there is a potential logic flaw related to locking/unlocking and protecting/unprotecting keys. The function - named rnp_key_unlock() - unlocks a key and has secret key material for use without password protection. This puts all values into memory so the key becomes usable for corresponding operations (e.g. changing attributes or exporting keys).

As an example, the flow of operations is as follows:

1. Unlock the key by invoking rnp_key_unlock()
2. Perform some operations on the key, e.g. export it by using rnp_key_export()
3. Lock the key again by invoking rnp_key_lock()

It was identified that the rnp_key_lock() might not be invoked in case the desired operation, in the example above rnp_key_export(), is running into an error. This situation potentially allows an attacker to perform operations on already unlocked keys, without needing to unlock them beforehand.

A similar pattern has been observed for rnp_key_protect/rnp_key_unprotect(), which gets invoked when keys are imported through importKeyBlockImpl(). A protected key is encrypted and can be safely held in memory. Invoking rnp_key_unprotect() on a given key removes the encryption from the key.

Affected File:
comm/mail/extensions/openpgp/content/modules/RNP.jsm

Affected Code:
refer to Attachment 9182160 [details]

Locking/protecting the keys in case an operation performed on an unlocked/unprotected key fails is important because it reduces the potential risk of having unlocked/unprotected keys in memory. Therefore, it is recommended to properly catch any occurring exceptions and re-lock/protect keys again.

Wayne Mery (:wsmwk) Reporter
Updated • 2 years ago

Assignee: o.nickolay → nobody
Summary: RNP-01-012 WP1 RNP: encrypt_secret_key() does not wipe keybuf from memory (Low) → RNP-01-012 WP1 Thunderbird: Logic issue potentially leaves key material unlocked (Medium)
Whiteboard: ~~[RNP]~~

Daniel Veditz [:dveditz]
Updated • 2 years ago

Keywords: sec-moderate

Magnus Melin [:mkmelin]
Updated • 2 years ago

Assignee: nobody → mkmelin+mozilla

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

I will attach a first revision of a fix, which is currently untested. I'm attaching it anyway, phabricator might help me self-review more easily.

The fix will affect the following actions. We need to test these actions still work correctly with the new patch.

- key generation
- import secret key
- backup secret key
- change expiration date

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

*Attached file **Bug 1673239 - OpenPGP key material should remain locked in memory in failure scenarios. r=mkmelin** — Details*

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

I've implemented automated tests for secret keys in ~~bug 1693554~~.
Tests pass without and with the fixes from this bug.

Magnus Melin [:mkmelin]
Updated • 2 years ago

Assignee: mkmelin+mozilla → kaie
Status: NEW → ASSIGNED
status-thunderbird_esr78: --- → affected
Target Milestone: --- → 87 Branch

Magnus Melin [:mkmelin]
Comment 4 • 2 years ago

https://hg.mozilla.org/comm-central/rev/b14afc010507d8d5857bc739dc75ed022e30792e

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

Magnus Melin [:mkmelin]
Updated • 2 years ago

tracking-thunderbird_esr78: --- → +

Magnus Melin [:mkmelin]
Comment 5 • 2 years ago

Comment on attachment 9203762 [details]
~~Bug 1673239~~ - OpenPGP key material should remain locked in memory in failure scenarios. r=mkmelin

[Approval Request Comment]
User impact if declined: sec issue
Testing completed (on c-c, etc.): on beta
Risk to taking this patch (and alternatives if risky): doesn't seem very high

Attachment #9203762 - Flags: approval-comm-esr78?

Wayne Mery (:wsmwk) Reporter
Comment 6 • 2 years ago

Comment on attachment 9203762 [details]
~~Bug 1673239~~ - OpenPGP key material should remain locked in memory in failure scenarios. r=mkmelin

[Triage Comment]
Approved for esr78

Attachment #9203762 - Flags: approval-comm-esr78? → approval-comm-esr78+

Rob Lemley [:rjl]
Comment 7 • 2 years ago

uplift

Thunderbird 78.8.1:
https://hg.mozilla.org/releases/comm-esr78/rev/0c8606e7f45d

status-thunderbird_esr78: affected → fixed

Wayne Mery (:wsmwk) Reporter
Comment 8 • 2 years ago

Kaie, will you be arranging a security advisory for this?

Flags: needinfo?(kaie)

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

Sorry for having missed this at the time of release. I will work with Tom to check if we can release a CVE late.

Flags: ~~needinfo?(kaie)~~

Tom Ritter [:tjr]
Updated • 2 years ago

Alias: CVE-2021-29950

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

Regressions: ~~CVE-2021-29956~~

Wayne Mery (:wsmwk) Reporter
Updated • 2 years ago

Group: ~~mail-core-security~~