

Copy Summary

View

Closed

Bug 1673241 (CVE-2021-29957)

Opened 2 years ago

Closed 2 years ago

RNP-01-008 WP3 Thunderbird: Partially unencrypted email insufficiently detected (Low)

Categories

Product: MailNews Core

Component: Security: OpenPGP

Version: 78

Type: defect

Priority: Not set

Severity: --

Tracking

Status: RESOLVED FIXED

Milestone: 90 Branch

Tracking Flags:

thunderbird_esr78

thunderbird89

Tracking

Status

+ fixed

+ fixed

People

(Reporter: wsmwk, Assigned: KaiE)

References

(Regressed 1 open bug)

Details

(Keywords: sec-low)

Attachments

Bug 1673241 - Improve handling of mixed MIME and inline OpenPGP. r=PatrickBrunschwig,mkmlin

2 years ago Kai Engert (KaiE)

48 bytes, text/x-phabricator-request

wsmwk : approval-comm-beta+

wsmwk : approval-comm-esr78+

Details

Review

Bottom

Tags

Timeline

Wayne Mery (wsmwk)

Reporter

Description • 2 years ago

It was found that a partially unencrypted email has been insufficiently detected as such by Thunderbird. This introduces the risk of users erroneously assuming the entire email was encrypted and therefore ascribing it with an incorrect security status.

*Proof-of-Concept .eml file:

refer to [Attachment 9182160 \[details\]](#)

It is recommended that the logic for detecting encrypted content receives improvements by design. If parts of the message were decrypted, the whole message should be checked for unencrypted parts. If any parts of the parts were not decrypted, the application should alert the user about partially unprotected information.

Daniel Veditz (dveditz)

Updated • 2 years ago

Keywords: sec-low

Kai Engert (KaiE)

Assignee

Comment 1 • 2 years ago

Alessandro: This is the bug I mentioned in [bug 4702502](#), FYI.

Kai Engert (KaiE)

Assignee

Comment 2 • 2 years ago

Adding Patrick to CC.

I'm working on several changes to the handling of inline messages.

Kai Engert (KaiE)

Assignee

Comment 3 • 2 years ago

Regarding the past EFAIL security issue, one of the remedies was to limit processing of encrypted messages to the top level of a MIME message.

Apparently this wasn't applied to messages that are a mix of MIME and inline PGP. In the provided sample, there are three MIME parts. One of them contains an inline PGP message, and our current code is willing to process it.

I think it is OK if we continue to allow processing of exactly one inline PGP message, even if it is contained in the second level of a MIME message. However, if we do, we should give it the "partial PGP" treatment. We should show the notification that it's partial. We shouldn't process it automatically, but require the user to click the button to process the partial content. And after the user clicks, we should hide all other MIME parts. (This is what we currently do for a single-part plain text message, which contains an PGP block.)

There is some existing code (which refers to a [bug 983](#)), which has this comment:

```
// for safety reasons, we replace the complete visible message with
// the decrypted or signed part (bug 983)
```

But that code doesn't work. For the given example, additional rendered content is kept.

Also, currently the code will always replace the first rendered MIME part with the decrypted/decoded contents - even if that isn't the PGP block.

We should change the code to walk the DOM and remove all unrelated DIV nodes.

Also, there is code that recursively processes the full MIME tree, and will decode any parts at any nesting level. We should remove that code for at least two reasons. (1) Our new code (post Enigmail) will use the result of decoding to update the top level message status and show status indicators, and we don't support displaying status for sub content. (2) Because of the risks described around the EFAIL security issues, we shouldn't automatically process sub content.

While testing, I discovered that for messages that we cannot process (cannot decrypt, e.g. because of a broken digest part), we will not show any OpenPGP failure status (because RNP doesn't give us an helpful error code). I suggest two changes here. (3) If we don't get helpful failure information, let's check if the message we're trying to process is an encrypted message or a signed message (according to its BEGIN PGP header), and show the respective general OpenPGP error status. (4) If we're processing partial contents, let's always reduce the shown contents. In other words, remove the code around it, and keep the PGP message that we cannot process. I've suggested this also in [bug 4702502](#).

Kai Engert (KaiE)

Assignee

Comment 4 • 2 years ago

Attached file [Bug 1673241 - Improve handling of mixed MIME and inline OpenPGP. r=PatrickBruschwig,mkmelin](#) — Details



Phabricator Automation
Updated • 2 years ago



Assignee: nobody → kaie
Status: NEW → ASSIGNED



Kai Engert (:KaiE:) Assignee
Comment 5 • 2 years ago



I have test messages for interactive testing, I'll work on automating in a separate patch.



Ronald Tse
Comment 6 • 2 years ago



Kai, RNP is happy to provide helpful response for a clean implementation on this case. If you remember, we do have a pending ticket that we need to discuss with your side on (1) the needs of TB from a compliance profile and (3) the interface between TB/RNP to describe the fit of a compliance profile. This in scope in the original project i.e. comes with a deadline from MOSS.



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



Ronald, most of this bug is about PGP/MIME. We don't use RNP to process the MIME structure of an email, we're using code in Thunderbird (formerly Enigmail code) to do that. I'm not sure how [comment-6](#) is related to this bug.



Ronald Tse
Comment 8 • 2 years ago



Got it, thanks for the clarification Kai!



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



<https://hg.mozilla.org/comm-central/rev/34b4c229c416a707188eb2dddf0698c7d1cd8fe11>

Status: ASSIGNED → RESOLVED
Closed: 2 years ago
[status-thunderbird_esr78](#): --- → affected
Resolution: --- → FIXED
Target Milestone: --- → 90 Branch



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



lint fix:
<https://hg.mozilla.org/comm-central/rev/1536dedb52da7b63fd7509d909a108504dd58bf8>



Magnus Melin (:mkmelin)
Updated • 2 years ago



[tracking-thunderbird89](#): --- → +
[tracking-thunderbird_esr78](#): --- → +



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



Comment on [attachment 9213156](#) [details]
[bug 1673244](#) - Improve handling of mixed MIME and inline OpenPGP. r=PatrickBruschwig,mkmelin

Needs testing on beta, because we should consider to uplift to 78.11

[Approval Request Comment]

Regression caused by (bug #): no

User impact if declined: imprecise OpenPGP status reports for some message

Testing completed (on c-c, etc.): yes

Risk to taking this patch (and alternatives if risky): mild risk for regressions, but passes existing tests, and we add new tests

[Attachment #9213156](#) - Flags: approval-comm-beta?



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



[status-thunderbird89](#): --- → affected



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



The fix assumes that the fixes from [bug 1701008](#), [bug 1702502](#), [bug 1701024](#) are present, so adding dependencies.

Depends on: [1701008](#), [1702502](#), [1701024](#)



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












Comment on [attachment 9213156](#) [details]
[bug 1673244](#) - Improve handling of mixed MIME and inline OpenPGP. r=PatrickBruschwig,mkmelin

See above beta approval request for details.

Requesting esr78 approval, however, should wait for at least 2 weeks beta testing.

[Attachment #9213156](#) - Flags: approval-comm-esr78?

 Wayne Mery (wsmwk) Reporter Comment 14 • 2 years ago	<div>—</div>
Comment on attachment 9213156 [details] Bug 1673244 - Improve handling of mixed MIME and inline OpenPGP. r=PatrickBrunschwig,mkmlin [Triage Comment] Approved for beta	
Attachment #9213156 - Flags: approval-comm-beta? → approval-comm-beta+	
 Kai Engert (KaiE:) Assignee Comment 15 • 2 years ago	<div>—</div>
https://hg.mozilla.org/releases/comm-beta/rev/beceab875bd723113c4bd0f3315fac584fd5062f89.0b3 status-thunderbird89 : affected → fixed	
 Wayne Mery (wsmwk) Reporter Comment 16 • 2 years ago	<div>—</div>
Comment on attachment 9213156 [details] Bug 1673244 - Improve handling of mixed MIME and inline OpenPGP. r=PatrickBrunschwig,mkmlin [Triage Comment] Approved for esr78	
Attachment #9213156 - Flags: approval-comm-esr78? → approval-comm-esr78+	
 Kai Engert (KaiE:) Assignee Comment 17 • 2 years ago	<div>—</div>
https://hg.mozilla.org/releases/comm-esr78/rev/d2f01d2934ed8aa63dafa946a90008f68c6daf0a78.10.2 status-thunderbird_esr78 : affected → fixed	
 Wayne Mery (wsmwk) Reporter Comment 18 • 2 years ago	<div>—</div>
Kai, if you plan to do a CVE for this issue, please coordinate with security@mozilla.com - we intend to release 78.10.2 on Monday or Tuesday. Flags: needinfo?(kaie)	
 Kai Engert (KaiE:) Assignee Comment 19 • 2 years ago	<div>—</div>
cve requested Flags: needinfo?(kaie)	
 Tom Ritter [tjr] Updated • 2 years ago	<div>—</div>
Alias: CVE-2021-29957	
 Wayne Mery (wsmwk) Reporter Updated • 2 years ago	<div>—</div>
Group: mail-core-security	
 Magnus Melin [mkmelin] Updated • 7 months ago	<div>—</div>
Regressions: 1770004	

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

Top ↑