### Tails - Feature #6156

**Upstream secure Thunderbird autoconfig wizard**

**Status:** In Progress  
**Start date:** 05/19/2016  
**Due date:**  

**Priority:** Normal  
**Due date:**  

**Assignee:** anonym  
**% Done:** 100%  
**Start date:**  

**Category:**  
**Estimated time:** 0.00 hour  
**Spent time:** 0.00 hour  
**Target version:** 2020  
**Feature Branch:** feature/6156-thunderbird-secure-auto-config  
**Starter:** No  
**Type of work:** Communicate  
**Affected tool:** Email Client  

**Description**

Get these patches merged in Thunderbird upstream.

Upstream merge request: [https://bugzilla.mozilla.org/show_bug.cgi?id=971347](https://bugzilla.mozilla.org/show_bug.cgi?id=971347)

**Subtasks:**

- **Bug # 11450:** Update the Icedove account setup wizard security patches according to what... **Resolved**
- **Bug # 15788:** Rethink our patches with Thunderbird 60 **Resolved**
- **Bug # 15790:** Thunderbird autoconfig does not respect the ISP's hints **Rejected**
- **Feature # 16147:** Re-import secure-account-creation patch series for thunderbird **Rejected**

**Related issues:**

- Related to Tails - Feature #6150: Help Tor people upstream the Torbirdy patches **Resolved**
- Related to Tails - Feature #7064: Update our plans for securing Icedove's aut... **Resolved**
- Related to Tails - Bug #15387: The Mozilla auto_config database requires an u... **Rejected**
- Related to Tails - Feature #16771: Upgrade to Thunderbird 68 **Resolved**
- Related to Tails - Bug #16856: Consider using non-Riseup email for Thunderbir... **Resolved**
- Related to Tails - Bug #17277: Check if the Thunderbird autoconfig wizard tru... **Confirmed**
- Blocked by Tails - Bug #11536: Icedove autoconfiguration is broken for ISPs s... **Resolved**
- Blocked by Tails - Bug #12151: Get Thunderbird's test suite running and test ... **Resolved**
- Blocks Tails - Feature #16209: Core work: Foundations Team **Confirmed**

**Associated revisions**

**Revision 8a9de848 - 08/26/2016 11:10 AM - anonym**

Pin Icedove to be installed from our APT repo.

Debian's Icedove packages still do not have our secure Icedove autoconfig wizard patches applied, so installing them would be a serious security regression.

Refs: #6156

Will-fix: #11613

**Revision 0d4b993c - 04/02/2018 01:49 PM - anonym**

Enable the feature-6156-thunderbird-secure-auto-config APT overlay.

Will-fix: #6156
Update Thunderbird prefs vs 52.7.0-1~deb9u1.0tails1+6156.

I.e. the first build with the rewritten secure auto config patch series applied.

And as a preparation for the upstream work in TorBirdy that will follow, let's set these prefs via a patch to TorBirdy.

Refs: #6156

Patch Thunderbird packages from Debian when building Tails images (refs: #16834, #6156).

This avoids the need to build and upload Thunderbird packages every now and then. Instead, we'll need to refresh our patches when they don't apply as-is anymore.

Current patchset imported from our icedove.git at commit a3eb1e85558f2c9cf01d332920ac81fe3cd9fd.

Thunderbird: disable unsafe automatic configuration methods.

While working on refs: #6156 it was forgotten to fix the configuration in Tails. Oops!

Will-fix: #17277

Thunderbird: disable unsafe MX automatic configuration method.

While working on refs: #6156 it was forgotten to fix the configuration in Tails. Oops!

Will-fix: #17277

Thunderbird: disable unsafe MS Exchange automatic configuration method.

While working on refs: #6156 it was forgotten to fix the configuration in Tails. Oops!
However, while working on refs: #17277 it was noticed that something seems buggy so this change will likely just break Thunderbird at the moment. To be investigated!

Will-fix: #17654

Revision 14821f72 - 04/27/2020 09:12 AM - anonym
Thunderbird: patch to fix buggy MS Exchange autoconfig pref.

When MS Exchange autoconfig is disabled via this pref, the account wizard breaks, making it useless. It seems the work in refs: #6156 did this. The added patch fixes this, and should be upstreamed.

Will-fix: #17654

History

#1 - 07/19/2013 07:08 AM - intrigeri
- Parent task set to #5663

#2 - 07/19/2013 07:08 AM - intrigeri
- Type of work changed from Wait to Code

#3 - 10/03/2013 11:09 AM - intrigeri
- Type of work changed from Code to Upstream
- Starter set to No

#4 - 10/03/2013 11:13 AM - intrigeri
- Subject changed from upstream secure Icedove autoconfig wizard to Upstream secure Icedove autoconfig wizard

#5 - 08/12/2014 01:43 PM - intrigeri
- Category set to 212

#6 - 09/22/2014 11:40 AM - intrigeri
- Type of work changed from Upstream to Code

#7 - 01/02/2015 07:29 PM - BitingBird
I think the type of work is communicate, since at least in Debian I see no big report, but I'm not sure so I let it as is for now.

#8 - 01/03/2015 11:17 AM - intrigeri
- Type of work changed from Code to Communicate

#9 - 05/29/2015 12:36 PM - intrigeri
- Assignee set to Anonymous
- Target version set to 246

#11 - 05/29/2015 12:40 PM - intrigeri
- Related to Feature #6150: Help Tor people upstream the Torbirdy patches added
#12 - 11/27/2015 04:45 AM - sajolida
- Target version changed from 246 to Tails_2.0

#13 - 12/22/2015 06:27 AM - Anonymous
- Target version changed from Tails_2.0 to Tails_2.4

#14 - 12/22/2015 07:00 AM - Anonymous
Setting realistic target version to 2.4, maximum latest delay would be 2.5.

#15 - 12/22/2015 09:33 AM - intrigeri
Today we discussed that this should be started during the 2.2 cycle, span over the 2.3 and 2.4 ones. I would suggest setting a milestone that matches when you should start working on it, instead of one that matches when it should be finished, to prevent any risk that it's forgotten until 2.3 is out. Your call, of course :)

#16 - 01/05/2016 03:06 PM - Anonymous
- Related to Feature #7064: Update our plans for securing Icedove's autoconfig wizard wrt. recent developments added

#17 - 01/09/2016 06:13 PM - Anonymous
- Status changed from Confirmed to In Progress
- % Done changed from 0 to 10

#18 - 01/09/2016 06:19 PM - Anonymous
The current plan is to send our patches with a text to Torbirdy people for a first review with ETA Jan 24th 2016.

Then ideally we would be able to send them to the Thunderbird people and also update the corresponding TPO ticket. I'd also open a Debian bug with the same patches and link it to the upstream bug, so eventually the patches could be included in Debian directly - until upstream has them released.

#19 - 02/27/2016 12:39 PM - Anonymous
I've posted the patches upstream today. See https://bugzilla.mozilla.org/show_bug.cgi?id=669238 and https://bugzilla.mozilla.org/show_bug.cgi?id=971347

#20 - 02/27/2016 12:51 PM - intrigeri
I've posted the patches upstream today.

Great! A link would be useful next time we need to report about the progress of this task :)

#21 - 05/16/2016 05:34 AM - anonym
- Blocked by deleted (Feature #6154: Secure the Icedove autoconfig wizard)
#22 - 05/24/2016 01:13 PM - Anonymous
- Blocks Bug #11481: Alert TorBirdy devs about Thunderbird upstream patch prefs added

#23 - 05/24/2016 01:45 PM - Anonymous
- Target version changed from Tails_2.4 to Tails_2.5

Unlikely that this will happen in time for 2.4. Postponing.

#24 - 06/07/2016 02:14 AM - Anonymous
- % Done changed from 10 to 20

There has been quite some progress. Our patches have all been reviewed now and only code style improvements were asked for as a result of this review. This makes me think that we're nearly there! We'll work on a modified patchset taking upstream's remarks into account later this week.

#25 - 06/07/2016 02:18 AM - intrigeri

There has been quite some progress. Our patches have all been reviewed now and only code style improvements were asked for as a result of this review. This makes me think that we're nearly there! We'll work on a modified patchset taking upstream's remarks into account later this week.

Excellent news, glad to read that!

#26 - 06/10/2016 06:19 AM - Anonymous
We've resubmitted a new patchset today which was thoroughly tested by anonym. Waiting for a reply from upstream now. Let's hope for the best.

#27 - 08/02/2016 04:39 AM - Anonymous
- Target version changed from Tails_2.5 to Tails_2.6

#28 - 08/18/2016 12:19 PM - Anonymous
- Blocked by Bug #11536: Icedove autoconfiguration is broken for ISPs serving a OAuth config added

#29 - 08/31/2016 05:11 AM - intrigeri
- Blocks Bug #11450: Update the Icedove account setup wizard security patches according to what'll be decided upstream added

#30 - 08/31/2016 05:13 AM - intrigeri
- Blocks deleted (Bug #11450: Update the Icedove account setup wizard security patches according to what'll be decided upstream)

#31 - 09/15/2016 07:47 AM - Anonymous
I've submitted the latest patchset today. Waiting for upstream again now.

#32 - 09/20/2016 04:53 PM - anonym
- Target version changed from Tails_2.6 to Tails_2.7
Repinged upstream today.

I think that this ticket's deliverable has been accomplished "try hard to upstream the icedove autoconfig wizard". Thus, we'll continue to keep track of it, but not as part of the deliverable.

---

I think that this ticket's deliverable has been accomplished "try hard to upstream the icedove autoconfig wizard". Thus, we'll continue to keep track of it, but not as part of the deliverable.

Woohoo! \o/

---

intrigeri wrote:

Woohoo! \o/

+1 :)
I suspect that you folks will have other, more urgent things to do until 3.0 is out, so setting target version to 3.1.

---

#41 - 09/05/2017 07:40 PM - Anonymous
- Target version changed from Tails_3.1 to Tails_3.3

#42 - 11/15/2017 11:30 AM - anonym
- Target version changed from Tails_3.3 to Tails_3.5

#43 - 01/07/2018 03:50 PM - intrigeri
I see lots of discussion happening on the corresponding upstream bug in the past three months. Someone posted an updated patch and somewhat aggressively engaged with upstream. Upstream reacted (very understandably) somewhat defensively. If we still plan to get this merged some day, I think we need to intervene and help de-escalate the situation. anonym & u, did you follow this discussion, do you plan to get involved? If not, please let me/us know that you need help there: I don't think we can afford doing nothing about it on the long term, the risk of having to ship our patched Thunderbird package forever is just too great. Thanks in advance!

---

#44 - 01/15/2018 11:23 AM - Anonymous
See https://labs.riseup.net/code/issues/6156#note-35 for why I am unblocking #8668.

---

#46 - 01/15/2018 11:25 AM - Anonymous
I will take care of the upstream discussion.

However, our patches have not been merged because we were unable to provide a version that worked in Thunderbird's test suite (which we did not manage to run). This is #12151.

#47 - 01/15/2018 11:27 AM - Anonymous
- Blocked by Bug #12151: Get Thunderbird's test suite running and test our patches added

---

#48 - 01/23/2018 07:52 PM - anonym
- Target version changed from Tails_3.5 to Tails_3.6

---

#49 - 02/26/2018 03:11 PM - Anonymous
I replied on the bug - there was a lot of activity recently and it seems like people are still willing to have these patches reviewed and incorporated into Thunderbird. See https://bugzilla.mozilla.org/show_bug.cgi?id=971347

---

#50 - 02/27/2018 11:11 AM - intrigeri
it seems like people are still willing to have these patches reviewed and incorporated into Thunderbird.

---

I wonder who these people are and whether I missed something because my understanding of the situation is very different, and still the same as #5156#note-43 (nothing happened since then anyway until your own comment): among the two Thunderbird maintainers who commented, one nack-ed and the other one has strong doubts). I see someone else (alta88) arguing and insisting in favour of our patches but I'm not sure that will help much, quite the opposite IMO.
intrigeri wrote:

it seems like people are still willing to have these patches reviewed and incorporated into Thunderbird.

I wonder who these people are and whether I missed something because my understanding of the situation is very different.

Looks like it.

and still the same as #6156#note-43 (nothing happened since then anyway until your own comment): among the two Thunderbird maintainers who commented, one nack-ed

I'm not sure what "nack'ing" is, may you please explain that?

and the other one has strong doubts).

This one says ”Of course SSL/TLS connections would be preferred” and “I see the patch add proxy support in some of the paths, maybe at least that part could be accepted?” So the way you phrase it (“strong doubts”) seems slightly pessimistic to me.

I see someone else (alta88) arguing and insisting in favour of our patches but I’m not sure that will help much, quite the opposite IMO.

Absolutely, but I sincerely hope Thunderbird people can make the distinction between this person, us, and the problem we’re trying to solve.
I'm not sure what "nack'ing" is, may you please explain that?

Sure, sorry! ACK = agreeing/approving != NACK = disagreeing/rejecting

and the other one has strong doubts.

This one says "Of course SSL/TLS connections would be preferred" and "I see the patch add proxy support in some of the paths, maybe at least that part could be accepted?". So the way you phrase it ("strong doubts") seems slightly pessimistic to me.

I think we'll have to agree to disagree on this one :)

I see someone else (alta88) arguing and insisting in favour of our patches but I'm not sure that will help much, quite the opposite IMO.

Absolutely, but I sincerely hope Thunderbird people can make the distinction between this person, us, and the problem we're trying to solve.

+1

---

TB now implements a cool feature which display a big red warning to users when they use insecure configs. Great! So all we have to do now, and anonym will do that next week, is to reduce our patches to the "prefer SSL over plaintext" and proxy parts and submit them again for review. Yaaay!
BTW, I’ve noticed that the Mozilla configuration database (https://live.mozillamessaging.com/autoconfig/v1.1/) often presents a CAPTCHA when the request originates from Tor => that method fails => 

#15387

---

#55 - 03/14/2018 11:32 AM - bertagaz
- Target version changed from Tails_3.6 to Tails_3.7

---

#56 - 04/02/2018 01:31 PM - anonym
- File secure-account-creation.tar.gz added
- Subject changed from Upstream secure Icedove autoconfig wizard to Upstream secure Thunderbird autoconfig wizard
- Assignee changed from anonym to Anonymous

Sorry for the delay, but this turned out quite a bit more work than expected. In the end, I actually go Thunderbird’s own automated test suite to work and now it passes with all patches applied!

Below you’ll find comments I’d like to prove to the reviewer. However, I’m unsure of what to do about patch 0018 now. The "red warning" is enough, IMHO, and if we and/or TorBirdy use the pref it adds, then most email over .onion-space will be impossible since they rely on end-to-end encryption/authentication provided by the .onion and do not provide SSL for the email protocols. If you agree, just remove patch 0018 and its comment below.

The previous approach of “one big patch” clearly failed, so let’s try an incremental approach with one patch per commit (besides now there are several bugfixes that IMHO deserves their own commits). Please review and merge this series up to the patch you are happy with; each commit is atomic and at most depends on earlier patches, so this is safe and makes sense, and we can return to the remaining patches later. In fact, in most cases if you dislike a particular patch you could just skip that one and at worst get a simple conflict in mailnews/mailnews.js when importing a later patch.

Here I provide some extra patch comments for the reviewer:

0001-Fix-the-prefilled-hostnames-for-manual-edit.patch
0002-Invalidate-config-when-restarting-autoconfiguration.patch
0003-Remove-buggy-debug-code.patch
0004-Fix-issue-when-mailnews.auto_config_url-is-empty.patch
0005-Document-that-mailnews.-auto_config-mx_service-url-.patch
0006-Comment-pref.patch

These are bugfixes and minor improvements which I suspect you’ll want to merge right away.

0007-Prefer-fetched-configurations-using-SSL-over-plainte.patch

There’s quite some effort made to prefer SSL in other places, so this is arguably a bugfix as well.

0008-Add-SOCKS-proxy-support-for-account-autoconfiguratio.patch

Fixes: https://bugzilla.mozilla.org/show_bug.cgi?id=669238

0009-Generalize.patch
0010-Fix-outdated-error-handling.patch
0011-Improve-logging-for-fetchConfigFromISP-during-autoco.patch

These are nice on their own, but builds up to the next patch:

0012-Fetch-ISP-configuration-using-SSL-if-possible.patch

This opportunistic attempt to prevent MitM can easily be worked around (attacker blocks https, thunderbird downgrades to http and the attacker wins)
but is better than nothing, and builds up to:

0013-Add-pref-to-force-SSL-for-ISP-fetch-during-autoconfi.patch

This adds an opt-in pref that fixes the above MitM completely.

0014-Add-pref-for-whether-we-accept-OAuth2-during-autocon.patch
0015-Use-overridden-user-agent-for-HTTP-s-during-autoconf.patch
0016-Add-pref-for-each-guess-timeout-during-autoconfigura.patch

These allows TorBirdy to greatly improve the autoconfiguration UX when using Tor.

0017-Improve-logging-of-guess-instances-during-autoconfig.patch

This one helped me debugging 0015 and 0016.

0018-Add-pref-for-whether-we-accept-plaintext-protocols-d.patch

Given the "red warning" that appears whenever a user tries to accept a plaintext protocol (see comment 127), this patch is not critical for us any more.

FWIW, I've seen the test-mail-account-setup-wizard.js test pass with all these patches applied.

#57 - 04/03/2018 05:49 PM - anonym

- Feature Branch set to feature/6156-thunderbird-secure-auto-config

#58 - 04/04/2018 11:33 AM - Anonymous

I added those to the upstream bug today.
Assignee changed from Anonymous to anonym

Forwarded Ben Buksch's review to anonym. Reassigning this ticket to you - feel free to reassign it to me later on.

Target version changed from Tails_3.7 to Tails_3.8

Target version changed from Tails_3.8 to Tails_3.10.1

I think #15788 should be done first thing before any more work is put into this project :)

Description updated

Assignee changed from anonym to Anonymous

QA Check set to Info Needed

Ulrike, one question for you at the bottom :)  

The recurring cost of maintaining & building custom Thunderbird packages a few times a year keeps piling up and it does not help make the FT sustainable. So at the summit I'll nominate this ticket for the roadmap + FT work, on the ground that it's become a serious maintainability hinderance and we've been waiting too long for the last mile to be walked based on good will and free time.

So let's sum up what we have. First, it looks like the patches are in good way to be upstreamed. We're pretty close! 

Second, things got more interesting recently and we now have three different patchsets:

- anonym's rebase of his original patchset, done in March 2018, on top of the upstream/60.0_b2 from Debian's Vcs-Git, that lives in the secure_account_creation-60.0_b2 branch of our Git repo; assuming kibi's refresh (see below) is OK, I think this one is merely of historical interest at this point
- kibi's refresh of the aforementioned patchset so that it applies on 60.0b10; that's what we currently have as a quilt patch series on our tails/stretch packaging branch and that was used to build debian/1%60.0_b10-1_deb9u1.0tails1 which whe'll ship in Tails 3.9~rc1; a more Git-friendly version lives on the secure_account_creation-60.0_b10 branch, based on the upstream/60.0_b10 tag from Debian's Vcs-Git
- anonym's improved patchset, that takes into account the last review done upstream in April 2018:
  - it was mistakenly based on Thunderbird 52.7 so probably needs a serious refresh
  - it is probably better (as in, closer to something that can be upstreamed eventually) than the other patchsets
  - AFAICT it was never published, let alone submitted upstream, so far; 4 people have access to it with the attached comments that explain things: anonym, Ulrike, kibi and myself (the 2 latter in <335bdf60-7be2-b0e3-9fbd-8a58db17e10d@451f.org>). Apparently anonym wanted the patches and the associated comments to go on the upstream bug report, so perhaps I could attach all this here to start with, so at least the material to submit is not kept secret, but there may be a reason why this did not happen yet. Ulrike?
AFAICT it was never published, let alone submitted upstream, so far; 4 people have access to it with the attached comments that explain things: anonym, Ulrike, kibi and myself (the 2 latter in <335bfd60-7be2-b0e3-9fd6-8a58db17e10d@451f.org>). Apparently anonym wanted the patches and the associated comments to go on the upstream bug report, so perhaps I could attach all this here to start with, so at least the material to submit is not kept secret, but there may be a reason why this did not happen yet. Ulrike?

It has not happened because it's not based on the current development version of TB, so these patches are very likely to be rejected - something I'd like to avoid, after all the complicated discussions we've gone through with upstream until now. And I was still expecting anonym to rebase the patches on a newer version of TB...

But yes, indeed, you can attach the patches here, and we can improve upon them from this point on. Please not the comments on the upstream bug: some patches have already been reviewed and are considered mergeably by them. If possible I'd like to add this in a comment somewhere, so that we don't redo work that has already been done.

#66 - 08/17/2018 06:25 AM - Anonymous
- Assignee changed from Anonymous to intrigeri
- QA Check deleted (Info Needed)

#67 - 08/17/2018 06:27 AM - Anonymous
I would love us to rework on these patches and resubmit them upstream for good. Let me know if you need my help for this or if FT will handle it from this point on.

#68 - 08/17/2018 06:29 AM - Anonymous
- Related to Bug #15387: The Mozilla auto_config database requires an unusable CAPTCHA for Torified requests added

#69 - 08/17/2018 12:28 PM - intrigeri

Let me know if you need my help

Anyone moving this forward is warmly welcome :) for this or if FT will handle it from this point on.

We'll see at the summit. In the current state of things I doubt the FT has the budget to do that.
u wrote:

But yes, indeed, you can attach the patches here, and we can improve upon them from this point on.

Note to myself: once this is done, set target version to 2019 and reassign to lamby, as per summit 2018.

lamby

Again, Did we discuss this? I don't recall doing so, thus just wondering if it's a mistake to assign it over to me specifically? (If it's "to be discussed" feel free to assign back - I note the "2019" target.)

intrigeri

Again, Did we discuss this?

Yes (but very briefly!) during the FT meeting when we were brainstorming the tasks we want to add to our roadmap for the next years. Here's what I remember: IIRC kibi expressed interest because he's already worked on our Thunderbird patched package, then I asked "how is your JavaScript", his answer suggested it would be better to assign the task to someone else, and after a show of hands you mentioned your JavaScript was OK. I probably jumped too fast to conclusions: the fact your JS is OK does not necessarily imply that you want to work on this specific task. Sorry! Either way, I think there's quite some info I need to share with you before you can tell whether you want to take it or not, so let's take this assignment with a grain of salt. If you prefer, feel free to de-assign yourself until we've had this conversation :)

intrigeri

- Assignee changed from intrigeri to lamby

intrigeri

- Assignee changed from lamby to anonym
- Target version deleted (Tails_3.10.1)

intrigeri

- Blocks Feature #16209: Core work: Foundations Team added

intrigeri

- Blocks Feature #15507: Core work 2019Q1: Foundations Team added

intrigeri

- Blocks Feature #16209: Core work: Foundations Team added
anonym has rebased our patches - once again - on the current code base of Thunderbird. I've posted them all to the bug at https://bugzilla.mozilla.org/show_bug.cgi?id=971347 (also see https://bugzilla.mozilla.org/show_bug.cgi?id=971347#c197 for explanations).

Let's hope that's the last time we need to do that.

This probably won't be completed in time for 3.13 but let's make it clear that this should be on top of your list of non-urgent tasks.

Thunderbird people are organizing a bugday. They have a document where they collect bugs to focus on:
https://docs.google.com/document/d/1jQfOIuu_9KYPw_hfrPiwGrhQWKy-bzBDr214_tstMbc/edit#
I've added "our" bug there.

Big news! Most patches have been upstreamed!

Summary of upstreamed patches
You can look here for reference

* Minor stuff:
  * Improve logging of guess instances.
  * Add comment for pref.
  * Invalidate config when restarting autoconfiguration.
* Tor compatibility
  * Add pref for setting the autoconfiguration guess timeout.
  * Add SOCKS proxy support for account guessing.
* Security

05/06/2020
- Also fetch ISP configuration using SSL.
- **New patch!** Add pref for guessing only SSL configs. (This is ~half of "Add pref for whether to accept plaintext protocols during autoconfiguration" that we will discuss below)

**Patches that are still not upstreamed**

**Make use of non-SSL Exchange AutoDiscover methods optional.**

Thunderbird very recently (60.6.0) added a new autoconfig method, Microsoft's AutoDiscover, which use two secure methods and one insecure HTTP fallback. On short notice I tried to secure it (i.e. only do the secure methods), but upstream didn't like it ("it breaks the protocol").

I propose we just disable this method entirely (mailnews.auto_config.fetchFromExchange.enabled → false).

**Add pref for whether we accept OAuth2 during autoconfiguration.**

This is pretty bad, UX-wise, which can be demonstrated in current Tails:

1. Start Thunderbird
2. Quit autotomail wizard
3. Flip mailnews.auto_config.account_constraints.allow_oauth2 to true
4. Start autotomail wizard for $account@gmail.com (must be a valid one that you have the password for)
5. Pick one of the two results (imap or pop, it doesn't matter) you get; due to its priority Mozilla's database will win, and its first pick is OAuth2 so that's what you get (it's not displayed unless you click the "Manual config" button)
6. A browser window will open, asking you to login to the Google account, so enter $account@gmail.com and its password
7. Observe the error message stating that you need to enable JavaScript
8. Closing that browser window brings you back to the result screen from step 5, but now it says "the username or password is wrong".

You are stuck in 8: autotomail will bring you exactly here again no matter what you try. Your only option is to click "Manual config" and change authentication from "OAuth2" to "Normal password" (both for pop/imap and smtp). Good luck! ;)

This breaks several providers, namely these Mozilla database entries that all employ OAuth2 as its first authentication option: gmail.com, google.com, googlemail.com, bk.ru, corp.mail.ru, inbox.ru, jazztel.es, list.ru, mail.ru. In addition to this any provider not in Mozilla's database that serve a .well-known config with OAuth2 first is also affected.

**Add pref for whether to accept plaintext protocols during autoconfiguration.**

This pref did two things:

1. When fetching configs, discard all configs using plaintext protocols
2. When guessing a config, only guess ssl protocols

If you look among the upstreamed patches you can see that the "new" patch adds a pref doing 2, so lets focus on 1.

1 is not so bad given that the upstreamed patch that makes us able to only fetch configs over ssl; an active attacked cannot inject a non-ssl config, so the provider must offer it. Let's say a provider offers only plaintext (I have never seen this in the wild) then when a user accepts its plaintext config the wizard will turn to a bit scary red warning explaining the problem, and requiring a confirmation that the user actually wants to proceed.

Personally I think this is good enough.

**Prefer fetched configurations using SSL over plaintext.**

In Tails we only fetch over SSL, so this means nothing to us. But it's a bit unfortunate for all other Thunderbird users. :/

**Next steps:**

1. Agree to just disable Microsoft AutoDiscover.
2. Discuss whether we are fine with only half of the "accept plaintext protocols" patch (i.e. the scary red warning is good enough).
3. Probably continue as usual (manual patching + attempt to upstream) with the OAuth2 patch.
4. ...
5. Celebrate?

05/06/2020
#92 - 06/01/2019 05:37 AM - intrigeri
- Related to Feature #16771: Upgrade to Thunderbird 68 added

#93 - 06/07/2019 01:22 PM - Anonymous
During our last meeting we decided that we still want to upstream the OAuth patch and apply anonym's proposal above, ie.

```plaintext
disable
mailnews.auto_config.fetchFromExchange.enabled = false
```

and disregard

**Prefer fetched configurations using SSL over plaintext.**
for Tails.

#97 - 06/19/2019 10:59 AM - anonym
(12:54:24) intrigeri: anonym: btw, wrt. the Thunderbird patch that they asked to file separately and we were not sure what was going on, I took a look
a couple weeks ago, and I think their reply is easy to understand in the context of the commit message of the patch they're referring to, which was a bit
unclear: it felt you were referring to other code that was not submitted yet (which is not the case AFAICT), so they asked to submit that other code.
(12:55:11) intrigeri: anonym: with this context in mind, I think their reply (based on a misunderstanding) makes sense. clarifying the commit message
should fix the misunderstanding, hopefully :)  

#98 - 06/25/2019 10:36 AM - anonym
anonym wrote:

(12:54:24) intrigeri: anonym: btw, wrt. the Thunderbird patch that they asked to file separately and we were not sure what was going on, I took a look
a couple weeks ago, and I think their reply is easy to understand in the context of the commit message of the patch they're referring to, which was a bit
unclear: it felt you were referring to other code that was not submitted yet (which is not the case AFAICT), so they asked to submit that other code.
(12:55:11) intrigeri: anonym: with this context in mind, I think their reply (based on a misunderstanding) makes sense. clarifying the commit
message should fix the misunderstanding, hopefully :)  

I think I get it. This is the problematic commit message:

Add pref for whether we accept OAuth2 during autoconfiguration.

For many providers JavaScript is required for OAuth2 to work; with it
disabled autoconfiguration then result in a terrible UX (e.g. the web
login fails, has to manually alter the authentication method). Let's
provide a pref that discards OAuth2 configurations so e.g. extensions
that disables JavaScript (like TorBirdy) can provide a workaround.

If I understand correctly the problematic part is "can provide a workaround". Ben understood it as something involving extra code for this
"workaround", but what I really meant was simply: "can provide autoconfiguration that doesn't fail get stuck and fail as soon as OAuth is presented as
a possible authentication method”.

#99 - 06/26/2019 09:19 AM - Anonymous
I opened a new bug for the OAuth issue here: https://bugzilla.mozilla.org/show_bug.cgi?id=1561542

#100 - 07/06/2019 10:57 AM - intrigeri
- Related to Bug #16856: Consider using non-Riseup email for Thunderbird automated tests added

#101 - 11/30/2019 07:35 PM - intrigeri
- Related to Bug #17277: Check if the Thunderbird autoconfig wizard trusts the result of DNS requests added

#102 - 12/13/2019 03:24 PM - hefee
@anonym: what is the current status of this issue? As the last notice was six months ago, it would be great to know the current state to decide how to go on.

#103 - 12/16/2019 12:43 PM - anonym
The only remaining thing is this: https://bugzilla.mozilla.org/show_bug.cgi?id=1561542
The reviewer is hesitant (yay...) but raised a possibly interesting point. Let me go through his full comment:

Magnus wrote:

Setting this pref opens up other problems though. You may have to set your (gmail etc) account to use "less secure applications", and without that you won't really be able to log in + no good indications of why.

Fair point, although of course still infinitely better than the current situation.

Maybe when we have several options, we could have them listed, and let the user change them if required.

This is already the case: you can click “Manual config” and then select any of auth methods from the two (IMAP/POP + SMTP) dropdoxes, but IMHO this does not qualify as a solution at all. This is not the path we want to take for auto-configuration.

And/or you could consider temporarily enabling the js during oauth.

Huh, yeah, maybe? This would give the ideal UX (e.g. GMail should work out of the box, without having to configure your account to accept "less secure applications") while only exposing Thunderbird to JavaScript shipped from hosts the user already trusts their email to (FWIW). If we also lock down JavaScript a bit (disable JIT etc) I think I'd be pretty confident. OTOH I don't think this should be default behavior -- others that disable JavaScript might not appreciate this and would then want a always_allow_javascript_for_oauth pref.

Thoughts?

I also got an alternative idea for the “old” patch: instead of introducing yet another pref we could just check if JavaScript is disabled, and if so also disable OAuth2.
Hi,

The only remaining thing is this: https://bugzilla.mozilla.org/show_bug.cgi?id=1561542

+ ensuring that our decisions from #6156#note-93 are tracked somewhere: for example, it seems that back then we decided to drop a couple patches, but we still carry them and segfault had to refresh them for Thunderbird 68. Will you file tickets for these things? If not, I'm happy to do this with my FT lead hat on.

I've no idea about what is cheap or expensive to implement so some of my ideas below may be too wild. You tell me! :)

The reviewer is hesitant (yay...) but raised a possibly interesting point. Let me go through his full comment:

tldr: I think having a pref that enables JS for OAuth2, even if it's otherwise globally disabled, is the best lead we have. It requires further investigation but it would 1. avoid some UX nightmares (the current one, and the one the patch replaces it with); 2. avoid having to write more code to mitigate these nightmares.

Magnus wrote:

Setting this pref opens up other problems though. You may have to set your (gmail etc) account to use "less secure applications", and without that you won't really be able to log in + no good indications of why.

Fair point, although of course still infinitely better than the current situation.

That's a strong statement. I understand you're saying that the resulting UX, in this situation, is infinitely better than the one you reported about when filing that ticket. Is this what you meant?

I did not test myself but what Magnus writes suggests to me that, from a user's perspective, it's essentially just as bad: at the end of the day, you can't read your email and you have no idea what to do to fix that. So I don't really understand what's "infinitely better". Maybe the path to failure is less painful? Anyway, this may not matter much, see below.

Maybe when we have several options, we could have them listed, and let the user change them if required.

This is already the case: you can click "Manual config" and then select any of auth methods from the two (IMAP/POP + SMTP) dropdoxes, but IMHO this does not qualify as a solution at all. This is not the path we want to take for auto-configuration.

I don't understand what the "several options" are in this context.

It looks like there are two different use cases:

- Folks who have never used their GMail account in Tails before: they'll have to log into their GMail account in a web browser, and do $stuff there, in order to get auto-config working. If we don't tell them they need to do that at the right time, auto-configuration does not seem to be an accurate description of their UX :/
- Folks who have already configured their GMail account for "less secure applications": in this case, I understand your patch does the right thing.

Problem is, Thunderbird can't tell in which situation it is without trying, right? Here as well, it may not matter much, see below.

And/or you could consider temporarily enabling the js during oauth.

Huh, yeah, maybe? This would give the ideal UX (e.g. GMail should work out of the box, without having to configure your account to accept "less secure applications") while only exposing Thunderbird to JavaScript shipped from hosts the user already trusts their email to (FWIW). If we also lock down JavaScript a bit (disable JIT etc) I think I'd be pretty confident.
IIRC, Torbirdy disabled JavaScript to protect against tracking and various kinds of infoleaks. These reasons certainly apply to HTML email and feeds coming from random places, but indeed, it could be that they don't apply in a context (OAuth2) where the user is logging in anyway. IMO this requires a more detailed analysis, but I'm optimistic, and I encourage you to dive deeper in this direction :)

OTOH I don't think this should be default behavior -- others that disable JavaScript might not appreciate this and would then want a always_allow_javascript_for_oauth pref.

Indeed, having JavaScript running when one has explicitly set the non-default pref("javascript.enabled", false); feels wrong.

I also got an alternative idea for the "old" patch:

I don't know what's the "old" patch, so bear with me if I got the following wrong.

instead of introducing yet another pref we could just check if JavaScript is disabled, and if so also disable OAuth2.

I understand it makes thing a bit more automatic outside of Tails (one still has to tweak their GMail account, but at least that's one less pref they have to learn about and to set), which seems like a very good idea to me! Software discovering how to behave by itself seems better, in principle, than adding prefs :). But I still prefer the idea of making OAuth2 Just Work™ even when JS is disabled globally.

In the context of Tails, it would have no impact (neither good nor bad) on the UX, right?

---

#105 - 02/11/2020 03:52 PM - anonym
- Target version changed from 2019 to 2020

Files

| secure-account-creation.tar.gz | 12.6 KB | 04/02/2018 | anonym |