Pidgin exposes everything through its D-Bus service

09/07/2017 07:01 PM - anonym

Status: Resolved
Priority: Normal
Assignee: % Done: 100%
Category: Estimated time: 0.00 hour
Target version: Tails_3.2
Feature Branch: bugfix/14612-deny-access-to-pidgin-dbus-service
Type of work: Code
Affected tool: Instant Messaging

Description
See e.g.: https://developer.pidgin.im/wiki/DbusHowto

So Tor Browser can totally sniff your buddy list and send your friends creepy messages.

Disabling this interface some how would solve this, but we're gonna use it in Tails Server's client application, to automate account creation, joining the right chat, etc. intrigeri tells me we could do D-Bus mediation with AppArmor once Linux 4.16 is available to us (unless it's delayed) which sounds ideal.

Related issues:
Blocks Tails - Feature #13234: Core work 2017Q3: Foundations Team

Associated revisions
Revision b2aabb12 - 09/13/2017 09:22 AM - intrigeri
Deny access to Pidgin's D-Bus service (refs: #14612).

That D-Bus interface is dangerous because it allows any application running as 'amnesia' that has access to the session bus to extract basically any information from Pidgin and to reconfigure it:
https://developer.pidgin.im/wiki/DbusHowto

Revision 565ed099 - 09/15/2017 02:44 PM - anonym
Test suite: workaround Pidgin's DBus interface being blocked.

We actually depend on it for some tests.

Refs: #14612

Revision fab65dc9 - 09/15/2017 02:48 PM - anonym
Test suite: Make sure Pidgin's DBus interface is blocked.

Refs: #14612

Revision dd12d608 - 09/15/2017 05:22 PM - anonym
Merge remote-tracking branch 'origin/bugfix/14612-deny-access-to-pidgin-dbus-service' into devel

05/15/2020
History

#1 - 09/07/2017 07:21 PM - anonym

Apparently there is a 5 year old (but unpublished?) CVE for this: [https://census-labs.com/news/2012/02/25/libpurple-otr-info-leak/](https://census-labs.com/news/2012/02/25/libpurple-otr-info-leak/)

Upstream ticket: [https://developer.pidgin.im/ticket/14830](https://developer.pidgin.im/ticket/14830)

I think it can be disabled with something like: DBUS_SESSION_BUS_ADDRESS= pidgin. Otherwise we could always recompile with --disable-dbus...

#2 - 09/10/2017 09:04 PM - intrigeri

I think it can be disabled with something like: DBUS_SESSION_BUS_ADDRESS= pidgin.

This would likely break input methods and a11y.

#3 - 09/11/2017 12:22 PM - intrigeri

I think we can forbid all access to that D-Bus interface via D-Bus "security policy" mechanism: see dbus-daemon(1) and e.g. /usr/share/dbus-1/session.conf.

#4 - 09/11/2017 12:25 PM - intrigeri

- Assignee set to intrigeri
- Target version changed from Tails_3.3 to Tails_3.2
- Type of work changed from Research to Code
- Affected tool set to Instant Messaging

#5 - 09/11/2017 12:25 PM - intrigeri

- Blocks Feature #13234: Core work 2017Q3: Foundations Team added

#6 - 09/11/2017 12:25 PM - intrigeri

(Seems more urgent than #12460 => replace it on my plate for this release.)

#7 - 09/13/2017 09:08 AM - intrigeri

- Subject changed from Pidgin exposes everything through its D-Bus interface to Pidgin exposes everything through its D-Bus service

Note to myself: dbus-send --session --print-reply --dest=im.pidgin.purple.PurpleService /im/pidgin/purple/PurpleObject im.pidgin.purple.PurpleInterface.PurpleAccountsGetAll returns exit code 0 iff. Pidgin is running and I am allowed to talk to its D-Bus service.

#8 - 09/13/2017 09:35 AM - intrigeri

- Status changed from Confirmed to In Progress
- Assignee changed from intrigeri to anonym
- % Done changed from 0 to 50
Thankfully that was trivial :) Once Tails Server has some kind of proper privileged backend / unprivileged frontend separation (\#12297) I expect it'll be feasible to give its backend access to the D-Bus interface without broadening the attack surface more than needed.

#9 - 09/15/2017 02:55 PM - anonym
- Assignee changed from anonym to intrigeri

Woah, apparently we're already using Pigin's DBus interface in the automated test suite, see 0bc56936a7134f6140df440dc1de042d9df9fada. Fixed with 565ed09904b7bbf59359f886cf4cf5d7cac4203.

I understand if you'd rather have me split that out into a separate branch/ticket for later. What do you think?

#10 - 09/15/2017 03:53 PM - intrigeri
- Assignee changed from intrigeri to anonym

LGTM

#11 - 09/15/2017 05:23 PM - anonym
- Status changed from In Progress to 11
- Assignee deleted (anonym)
- % Done changed from 50 to 100
- QA Check changed from Ready for QA to Pass

#12 - 09/28/2017 06:50 PM - anonym
- Status changed from 11 to Resolved