Ensure Tails is not affected by BlueBorne

Status: Resolved
Priority: Elevated
Assignee: intrigeri
Category: Security Audit
Target version: Tails_3.2
Feature Branch: bugfix/14655-disable-bluetooth
Type of work: Security Audit
Blueprint: https://security-tracker.debian.org/tracker/CVE-2017-1000251 (Linux kernel) +

Description

Related issues:
Related to Tails - Bug #14957: Document how to re-enable Bluetooth in the GNO... Confirmed 11/11/2017
Blocks Tails - Feature #13234: Core work 2017Q3: Foundations Team Resolved 06/29/2017

Revision e9f8fd1 - 09/14/2017 08:57 AM - intrigeri
Block loading of Bluetooth kernel modules (refs: #14655).

Revision 0329469f - 09/14/2017 08:57 AM - intrigeri
Block Bluetooth devices with rfkill (refs: #14655).

Revision 9320ca76 - 09/14/2017 09:04 AM - intrigeri
Update doc wrt. Bluetooth now disabled for real (refs: #14655).

Revision 1da7f2ec - 09/15/2017 05:22 PM - anonym
Merge remote-tracking branch 'origin/bugfix/14655-disable-bluetooth' into devel
Fix-committed: #14655

History
#1 - 09/14/2017 07:24 AM - intrigeri
We're not affected by CVE-2017-1000250 as we don't ship the BlueZ SDP server so I'll now focus on the Linux kernel vuln.

Our current kernel is affected by CVE-2017-1000251 i.e. remote (being in proximity to a vulnerable system) code execution in kernel space as long as bluetooth.ko is loaded. Red Hat says that CONFIG_CC_STACKPROTECTOR=y and CONFIG_CC_STACKPROTECTOR_STRONG=y make this vulnerability hard, but perhaps not impossible to exploit. My take on this is that it's good enough to avoid releasing an emergency Tails 3.1.1, so I'll focus on fixing this in Tails 3.2 instead.

The fix has been committed to the sid branch of src:linux and will be in 4.12.12-3. Presumably this will be uploaded at some point between now and the time we build the Tails 3.2 ISO. If this happens after 3.2-rc1 (very likely) we'll need to use our freeze exception mechanism to get this update, which is not much fun but totally doable. I can check with Ben and Salvatore to ensure their upload timeline works with our release schedule, but first I want to check if a more radical approach is doable.

I wonder if it's worth keeping Bluetooth kernel modules in Tails:

- the Bluetooth kernel stack may have other critical remotely exploitable vulns;
- Bluetooth devices have a unique 48-bit MAC address, that we don't spoof; I don't know if it's exposed in the air in current Tails;

... so if we can afford it UX-wise, some defense in depth would be great. Red Hat's mitigation instructions (Resolve tab) recommend setting up modprobe config to forbid loading the bnep, bluetooth and btusb kernel modules. On #10801 we are considering rfkill block bluetooth on top of that.

Let's now check how this would impact UX. Here's the current state of our Bluetooth support:

- The corresponding kernel modules are auto-loaded and we rfkill unblock bluetooth in config/chroot_local-includes/usr/local/lib/tails-set-wireless-devices-state, so once the userspace tools are installed Bluetooth should work.
- We don't ship the userspace tools (BlueZ, gnome-bluetooth) so Bluetooth cannot be used by default. One could add them to their Additional Software Packages, which should work e.g. for Bluetooth speakers, but as these packages are installed post-Greeter that won't help when ones needs Bluetooth to log in (e.g. when using a Bluetooth keyboard). In theory our long-term plan is #10801. But until we support persisting (in cleartext) Greeter settings, this won't work for using a Bluetooth keyboard in the Greeter.
- https://tails.boum.org/doc/advanced_topics/wireless_devices/ says "Bluetooth is enabled by default but Tails lacks the GNOME utilities to actually use it"; it also has hidden text (added in 4fa1c462fa0c70c7764d49be4812497815e2b32, commented out in 613b14c689c985d94361e90b0f696e3d2f7deaf9 because it was not up to our doc standards).

To sum up, we currently have no officially supported / documented way to make Bluetooth work, and power users who know how to get it working will only be able to use Bluetooth post-login (e.g. speakers) and not for what seems to be the most important use case to me (keyboard to enable persistence or admin password in the Greeter).

So disabling Bluetooth entirely should only harm a very limited amount of users, who do something we don't document/support, and for (what looks like) non-critical use cases only. I think we should do it now and maybe some day we'll add Bluetooth support for real (#10801).

I'll prepare a branch and will ask opinions around.
In passing, [#6457](#note-22) taught us that between 2014 and 2017-03, 30% of the WhisperBack reports we’ve received came from a machine with the bluetooth kernel module loaded. This gives us an idea of the amount of Tails users exposed to vulnerabilities in the kernel Bluetooth stack.

---

**#4 - 09/14/2017 09:05 AM - intrigeri**

- Feature Branch set to bugfix/14655-disable-bluetooth

---

**#5 - 09/14/2017 09:27 AM - anonym**

intrigeri wrote:

To sum up, we currently have no officially supported / documented way to make Bluetooth work, and power users who know how to get it working will only be able to use Bluetooth post-login (e.g. speakers) and not for what seems to be the most important use case to me (keyboard to enable persistence or admin password in the Greeter).

So disabling Bluetooth entirely should only harm a very limited amount of users, who do something we don’t document/support, and for (what looks like) non-critical use cases only. I think we should do it now and maybe some day we’ll add Bluetooth support for real [#10801].

---

I agree; I completely fail to see how the (currently) very unclear/limited benefits of keeping Bluetooth support (in its current state) around could justify the very clear risks (and uncertain ones, e.g. MAC tracking). However, I think we should just blacklist the modules (probably re-using the code from config/chroot_local-hooks/80-block-network) so power users that need Bluetooth support can re-enable it at their own risk (and a helpful tails-unblock-bluetooth script should be a single line if we want to be really nice).

---

**#6 - 09/14/2017 09:39 AM - intrigeri**

- % Done changed from 10 to 20

If my branch works fine on Jenkins I’ll submit it for QA so that 3.2~rc1 is safe vs. BlueBorne. And then, depending on the outcome of the discussion about the [proposal I’ve sent to tails-ux@](mailto:tails-ux@) we can either keep it or revert it for 3.2 (if the latter, we will have to pull a Linux kernel that fixes BlueBorne; if the former, we can choose).

---

**#7 - 09/14/2017 09:47 AM - intrigeri**

(and a helpful tails-unblock-bluetooth script should be a single line if we want to be really nice).

---

I’ve added the exact command lines that are needed in the commented out doc session about enabling Bluetooth, so that whoever picks up the task of documenting how to re-enable Bluetooth can use them or ask us to put them into a script. But I won’t dare touching that piece of doc myself, and don’t want to block on it.
#8 - 09/14/2017 01:29 PM - intrigeri
  - Assignee changed from intrigeri to anonym
  - % Done changed from 20 to 30
  - QA Check set to Ready for QA

Test suite (non-fragile tests) passed on my Jenkins, please review, merge & reassign to me so I can handle the next steps (possibly on another ticket, I'll see).

#9 - 09/15/2017 05:24 PM - anonym
  - Status changed from In Progress to 11
  - Assignee deleted (anonym)
  - % Done changed from 30 to 100
  - QA Check changed from Ready for QA to Pass

#10 - 09/28/2017 06:49 PM - anonym
  - Status changed from 11 to Resolved

#11 - 11/11/2017 01:07 PM - intrigeri
  - Related to Bug #14957: Document how to re-enable Bluetooth in the GNOME session added