issuetracker.google.com

# other in ExposureNotification [158932441] - Visible to Public

30-38 minutes

- **ap...@google.com <ap...@google.com> #1Jun 14, 2020 09:43AM**

  Created issue (on behalf of daughter-of-v@protonmail.com).
  09:43AM
  Summary: CVE-2020-13702: catastrophic breach of user privacy in Apple/Google COVID-19 Exposure Notification API

  Steps to reproduce:

  See detailed CVE description at https://github.com/normanluhrmann/infosec/raw/master/exposure-notification-vulnerability-20200611.pdf

  Browser/OS: Apple/Google ExposureNotification Architecture Vulnerability

  --

  have been requested to report here via ExposureNotificationServer github team

Attack scenario:
See detailed attack vector elaboration in https://github.com/normanluhrmann/infosec/raw/master/exposure-notification-vulnerability-20200611.pdf

Apple/Google must remove all ExposureNotification consumer apps from the store until Bluetooth LE vulnerability detailed above is rectified.

Due to the loss of Bluetooth LE Smart Privacy device tracking is possible by any Bluetooth receiver.

I have already published the issue because of the specific ramifications of this issue in context of GDPR: as Google is a data processor and ExposureNotification consumer app is a data controller both are considered fineable by conflict with GDPR - and affecting all ExposureNotification consumer app users world wide..

09:43AM
Reporter:

daughter-of-v@protonmail.com (Norman Luhrmann)
09:43AM
+CC:wo...@google.com, daughter-of-v@protonmail.com (Norman Luhrmann)

09:43AM
Type:Customer Issue

09:43AM
Title:other in ExposureNotification

- **ap...@google.com <ap...@google.com> #2Jun 14, 2020**

**09:43AM**

09:43AM

*NOTE: This e-mail has been generated automatically.*

Thanks for your report.

This email confirms we've received your message. We'll investigate and get back to you once we've got an update. In the meantime, you might want to take a look at the list of frequently asked questions about Google VRP.

If you are reporting a security vulnerability and wish to appear in Google Security Hall of Fame, please create a profile.

You appear automatically in our Honorable Mentions if we decide to file a security vulnerability based on your report, and you will also show up in our Hall of Fame if we issue a reward.

**Note that if you did not report a vulnerability, or a technical security problem in one of our products, we won't be able to act on your report. This channel is not the right one if you wish to resolve a problem with your account, report non-security bugs, or suggest a new feature in our product.**

Cheers,
Google Security Bot

Follow us on Twitter!

- **jk...@google.com <jk...@google.com> #3Jun 15, 2020 06:16PM**

  Status: Won't Fix (Intended Behavior)

  06:16PM
  Hey,

  Thanks for your bug report and research to keep our users secure! We've investigated your submission and made the decision not to track it as a security bug.

We believe your concern is addressed by the explicit requirement stated in the specification as follows:

“The advertiser address, Rolling Proximity Identifier, and Associated Encrypted Metadata shall be changed synchronously so that they cannot be linked.”
(Section "Broadcasting Behavior", page 5, Exposure Notification Bluetooth Specification, v1.2, https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf)

If you are aware of a deviation from this specification in the Android implementation of the protocol, please do let us know.

06:16PM
Status:New Won't Fix (Intended Behavior)

- **Norman Luhrmann <daughter-of-v@protonmail.com>**
  #4**Jun 16, 2020 11:47AM**

Dear team, I understand your point but please consider that the specification is in direct contradiction between my description of the rolling timer definitions and this remark about synchronous rotation.

Note that I have now traced the Bluetooth announcements on a Samsung Galaxy S10 with the German RKI Corona Warn app, and as I suspected the *GOOGLE PLAY

SERVICES* implementation does also not adhere to synchronous rotation.

Please see attached screenshot for rotation scenario where MAC changes but ServiceData does not. This is exactly the breaking scenario which renders Bluetooth LE Smart Privacy moot.

Please reopen this ticket and FIX THIS ISSUE.

I have also reported to Apple and will now update the CVE with your remarks and my new findings. Please handle this issue transparently and according to the ramifications of the potential rollout scale.

Thanks and BR, Norman

cve-rolling-id-collision.png

- **ap...@google.com <ap...@google.com> Jun 16, 2020 11:47AM**

- **Norman Luhrmann <daughter-of-v@protonmail.com> #5Jun 16, 2020 12:34PM**

- **Norman Luhrmann <daughter-of-v@protonmail.com> #6Jun 16, 2020 12:36PM**

  Also note that while I take no action for now I would like to let you know that this is already a violation with GDPR terms as it stands right now. Let's be reasonable in handling this thing.

- **ev...@google.com <ev...@google.com> #7Jun 16, 2020 01:15PM**

  Status: Accepted (reopened)

  01:15PM
  Hi,

  🎉 **Nice catch!** I've filed a bug based on your report.

  The panel will evaluate it at the next VRP panel meeting and we'll update you once we've got more information. All you need to do now is wait. If you don't hear back from us in 2-3 weeks or have additional information about the vulnerability, let us know!

  Regards,
  Eduardo', Google Security Team

  01:15PM
  Status:Won't Fix (Intended Behavior)     Accepted

  Assignee:<none>

  wo...@google.com

- **ap...@google.com <ap...@google.com> Jun 16, 2020 01:15PM**

**Norman Luhrmann <daughter-of-v@protonmail.com> #8Jun 16, 2020 03:10PM**

Glad I could help, it eases me greatly that this vector will be given a look at. Looking forward to your followup, glad I could help. BR

- **ap...@google.com <ap...@google.com> Jun 16, 2020 03:10PM**

- **ev...@google.com <ev...@google.com> #9Jun 16, 2020 03:45PM**

  hi we have a couple questions:

1. which phone mark/model did you use? and which OS.
2. the screenshot you showed shows the RPI reused across different MACs but were you able to see two different RPIs with the same MAC as well?

-

  **Norman Luhrmann <daughter-of-v@protonmail.com> #10Jun 16, 2020 05:18PM**

  Samsung Galaxy S10<br>
  One 2.0<br>
  Android 10<br>
  Kernel 4.14.113-17806689<br>
  Build QP1A.190711.020.G973FXXS4BTB3

  ad 2.: I only covered approx. 20 min in the scan which observed a single MAC rotation which did rotate the RPI at the same time. The device would need to be monitored for a longer duration to ensure that rotation always works in this direction.

- **Norman Luhrmann <daughter-of-v@protonmail.com>** #11**Jun 16, 2020 05:28PM**

  I wrote this in reverse, obviously I observed a single rotation of RPI which did properly rotate MAC too.

  Please note that the risk of device tracking is still very likely because with the exception of devices just leaving the scanner coverage area any "new MAC/RPI tuple" in the subsequent announcements - with an obvious statistical uncertainty that  is probably negligible in many real world traffic scenarios (# of announcers in range, movement of announcers, etc.).

  I stand by my observation that only a derivative and/or reuse of the MAC address seems a feasible solution. Fixing both directions would be an improvement to the issue above, but the same statistical analysis still allows the likely tracking of devices even in that case.

  BR

- **ev...@google.com <ev...@google.com>** #12**Jun 16, 2020 06:26PM**

Hi
Thanks for testing. We also tested this on our side, and confirmed that the
MAC always rotates when the RPI rotates. Glad we have the same results. I
believe now we both are seeing the same behavior.

In the latest scenario described in your previous message, identifying when
the RPI rotates and then follow it, the attackers goal would be to maintain
a database of RPIs likely belonging to the same users, I assume.

In which situations do you expect this to be problematic for user privacy?
Would this challenge any of the privacy commitments provided in the blog
posts, white papers or UI of the German app?

By the way, we would appreciate it if you could clarify your advisory about
the rotation of RPI always rotating the BT MAC, as to be technically
correct, as otherwise we end up contradicting each other in public :-)

Thank you!

- **Norman Luhrmann <daughter-of-v@protonmail.com>**

### #13Jun 16, 2020 08:08PM

Hi

I have uploaded an updated CVE and requested MITRE to switch the reference.
https://github.com/normanluhrmann/infosec/raw/master/exposure-notification-vulnerability-20200616-2.pdf

The fundamental issue with this vulnerability is the loss of Bluetooth LE Smart Privacy which is designated to protect this situation from happening.

The German Corona Warn app is under the jurisdiction of the European Union and thus held accountable for GDPR violations.

The situation that BT advertisings that are designated for peer mobile devices using the same framework are also processable by Bluetooth Beacons that happen to be in immediate vincinity presents a huge problem in that regard.

The following GDPR clauses are applicable to full or in part extent to this situation:
art 5: broad violation, transparency, etc
art 6. consentual processing not given
art 12-23: app user can not utilize her GDPR rights against beacon operators (e.g. right to be forgotten)
art 24: generic breach
art 25: breaking smart privacy does not encourage "data protection by design/default"
art 28: since every beacon operator processing the BT advertisings is legally considered a data processor this is a

major issue

the list goes on, the GDPR vs Bluetooth beacon topic is shockingly open to attack unless Google/Apple can ensure that no information leakage is to be expected under any circumstances.

most public discourse on the matter of app and data privacy is concerned with exactly such matters.. the situation is not without immediate danger for Google/Apple because from my PoV you are directly risking fines in case of a data protection agency picking up the matter.

my recommendation would be to deactivate any app live with ExposureNotification in the EU member markets, this issue is not limited to German RKI Corona Warn app.

BR

- **ev...@google.com <ev...@google.com> #14Jun 16, 2020 08:32PM**

Thanks for updating your report. I think the latest update is technically
correct.

Can you elaborate on how the rotation of the MAC address compromises
privacy?

It seems to me like the MAC address is being rotated more often than
necessary, why is this a problem?

We may be missing some attack scenario that you are seeing.

Also, please keep this discussion technical, our team is not allowed to
make legal conclusions or speculation, so it'll make it impossible for us
to answer or address any of your comments in that regard. Trust we want to
do the right thing, not because of regulations, but because we care.

- **Norman Luhrmann <daughter-of-v@protonmail.com>**
  #15**Jun 16, 2020 09:56PM**

The issue is not any potential extra MAC rotations but that for the duration that a phone advertises a stable RPI (approx 15 min) any other BT device in range can associate along MAC rotations that take place during that interval. This impacts Bluetooth Smart Privacy.

Given that currently the other direction properly dual rotates (dependent on signal timings) this makes a device loose privacy for something inbetween 15-30 minutes.

So when I am an ad beacon network operator I can now track a mobile device for up to half an hour of travel through an urban area simply by looking at my Greylog. Hello privacy laywers.

If I am an advanced actor I can easily massage the data with some learning algorithm to reassociate most of the "properly" working dual rotations due to beacon proximity/lateral movement. Hello Russia/China.

You should realize that there are currently 25 billion IoT devices of which many can be considered barely supported and security hardened 24/7 internet-connected hosts. Hello botnet operators.

I am defending this position because the reality is that an Exposure Notification framework with sub-second advertising interval is broken in a world of non-conforming data processors sitting at every ad display, security camera and public transport vehicle - regardless of GDPR implications.

The current status quo worsens this position by extending the time of trackability beyond what might be native Bluetooth stack rotation intervals due to RPI correlation.

Please see my PDF for details. https://github.com/normanluhrmann/infosec/raw/master/exposure-notification-vulnerability-20200616-2.pdf

- **ev...@google.com <ev...@google.com> #16Jun 16, 2020 11:14PM**

  11:14PM
  OK, Thanks for the clarification. Unfortunately before moving forward I need to make sure we both agree on the technical significance and privacy impact of the extra MAC rotations.

The PDF, on the Vulnerability Details section mentions that the problem described is about the interaction between the MAC and the RIP. Crucially, there is this quote in the PDF:

> *Both Bluetooth Smart Privacy address randomisation and Exposure Notification identifier rotation work as expected independently,* ***but anyone holding both data points can trace devices across rotations***.

I believe that now we agree that the identifier rotation works as expected, and I think we now agree that someone can't use the MAC for tracking, only the RIP. Is this correct? I just want to make sure we agree that the MAC has nothing to do with the report anymore, because the PDF still mentions it. The PDF still says:

> *[...] in the other direction the dual rotation is not applied as per specification guidance.*

Do you consider that a problem? Is there an attack with the MAC that we have not seen? Or is the concern uniquely related to the RPI?

I want to make sure we are 100% clear that we have moved past the extra MAC rotations, and are now only talking about the RPI. Can you please confirm that you agree that the extra MAC rotations are not a problem? Because the PDF update still make it sound like they are a problem, so I want to make sure we agree they are not.

**Norman Luhrmann <daughter-of-v@protonmail.com>**

### #17Jun 17, 2020 05:45AM

> I believe that now we agree that the identifier rotation works as expected, and I think we now agree that someone can't use the MAC for tracking, only the RIP. Is this correct?

This is correct

>> [...] in the other direction the dual rotation is not applied as per specification guidance.
> Do you consider that a problem?

Yes, since rotating the RPI along with a MAC rotation issued by the Bluetooth LE Random Device Address would decrease the tracking potential/increase the difficulty to implement tracking.

I think the subvectors can be classified as follows:

1. MAC address can be used for device tracking: not applicable to your implementation since RPI rotation properly rotates MAC at the same time.
2. RPI address can be used for device tracking: this is the current status of your implementation; since a random private address rotation does NOT properly rotate the RPI at the same time.
3. Hypothetical: if both MAC and RPI address ALWAYS rotate in tandem the easy device tracking explained in my whitepaper is no longer possible. ExposureNotification still suffers from reduced device tracking capabilities due to the constant high frequency advertising, but at least the metadata is no longer of any help.

I hope this clarifies things. I will gladly summarize our findings in another whitepaper update when you think we found a common agreement on a description of the issue. From my PoV:

1. OK in the implementation, NOT OK in the Bluetooth spec timer descriptions which are kind of contradictory between the plain timer interval descriptions and your remarked statement. A "Rotate timer A and B always together" description sure could be formed in a clearer fashion.
2. NOT OK in the implementation: should be fixed for a minimal vector mitigation to satisfy the CVE
3. Not relevant for the CVE at hand, I just add this to make you understand that I would still consider turning mobile phones into 24/7 high frequency advertising beacons a privacy issue, but certainly of reduced scope and increased abuse effort/complexity.

Feel free to ignore 3. in this ticket handling. I encourage a general discussion of this topic in context of GDPR though because I think the data processor status of IoT beacon operators is highly conflicting. This should not concern the implementation of ExposureNotification though, but - in addition to the highly disputed proximity detection accuracy - is the reason why I would presonally not see the cost/benefit ratio of ExposureNotification privacy as a deal worth making in any case.

Postscriptum: Note that I have not tested the Apple IOS implementation in the same fashion yet, but they are also informed (and as per my recommendation maybe in touch with you already).

- **ap...@google.com <ap...@google.com> Jun 17, 2020 05:45AM**

- **ev...@google.com <ev...@google.com> #18Jun 17, 2020 11:14AM**

11:14AM
Hi!

Perfect, thank you.

> [...] rotating the RPI along with a MAC rotation issued by the Bluetooth LE Random Device Address would decrease the tracking potential/increase the difficulty to implement tracking.

This sounds right.

1. > MAC address can be used for device tracking: not applicable to your implementation since RPI rotation properly rotates MAC at the same time.

Great! =)

2. > RPI address can be used for device tracking: this is the current status of your implementation; since a random private address rotation does NOT properly rotate the RPI at the same time.

To rephrase this point slightly, RPI rotates less frequently than the MAC, which means that the MAC provides better tracking protection than the RPI. I've added this to our internal bug report, so we can track this concern.

This could be resolved by making the RPI rotate more often than the MAC, but this has severe consequences on performance (I think this means phones would have to store more RPIs than today, which would result in longer time to do the matching on who has been exposed). This is ultimately a speed/computation trade-off with privacy.

I don't know where the 15mins metric came from, but maybe it can be changed, we'll see.

3. > Hypothetical: if both MAC and RPI address ALWAYS rotate in tandem the easy device tracking explained in my whitepaper is no longer possible. ExposureNotification still suffers from reduced device tracking capabilities due to the constant high frequency advertising, but at least the metadata is no longer of any help.

Thanks, that makes sense!

- **Norman Luhrmann <daughter-of-v@protonmail.com>**
  #19**Jun 17, 2020 03:46PM**

  Have you considered utilizing the MAC address in place of the RPI in Exposure Notification? I might miss something but FWIW I would assume that since the BT random device address already provides a rolling identifier not permanently associated to device/user there would be no purpose for a secondary one on BT devices supporting address randomization.

Either reusing the MAC address in the Exposure Notification protocol (given that BT address randomization is cryptographically sound) or putting a cryptographic derivative into the payload (if better randomization is required) would remove the problem.

That way you could avoid any issue caused by correlating datum carrying over. Feel free to ignore this, it might be stupid for reasons I do not see (legacy compatibility, etc.); just what I had in mind when I reviewed the spec.

- **ap...@google.com <ap...@google.com> Jun 17, 2020 03:46PM**

- **ev...@google.com <ev...@google.com> #20Jun 17, 2020 04:10PM**

  04:10PM
  Hi

  I was thinking the same, but I think we need a way to generate the RPIs based on a secret, and MACs are just random. It seems like the goal here was to achieve the privacy and health goals, and that seems to require control in the generation of the identifiers.

  By the way, we have made some progress on researching the reason why the RPI rotates every 15 minutes, and why the MAC is not rotated:

1. BLE MACs are rotated in average every 15 minutes (at random or static intervals, depending on the phone).

2. RPI s rotated in average every 15 minutes (at random intervals).

   As such, 50% of the time, the BLE MAC will rotate faster than the RPI, and the other 50% of the time the RPI will be faster. Since they are at different intervals, the "tracking protection" only happens on RPI, and doesn't happen with the MAC rotation (as you explained).

   However, I think that since the RPI rotates as frequently as the MAC (avg 15 mins), the tracking protection provided is equivalent.

   In other words, given that every RPI issuance is "fresh" from other identifiers (since we rotate the MAC every time there's a new RPI), the privacy guarantees are equivalent in both cases (assuming that the phone also rotates every 15 minutes).

   I looked around a bit, and I think that all phones rotate every 15 minutes, so this explains why the RPI rotates every 15 minutes. The goal seems to be simply to provide the same privacy guarantees as BLE.

- **ap...@google.com <ap...@google.com> #21Jun 17, 2020 04:27PM**

- **ev...@google.com <ev...@google.com> #22Jun 17, 2020 04:36PM**

  Status: Won't Fix (Intended Behavior)

  04:36PM

We just confirmed this with the Android team.
There are 2 different paths here. On Android R, we rotated the MAC in less than (but up to) 15 minutes, before R we rotate it at around 15 minutes.

For Exposure Notification, we rotate the RPI between 10-15 minutes. This means that in both paths above, there is a chance where either the MAC rotates before the RPI, or the RPI rotates before the MAC. In R, the chance is significantly higher that the MAC rotates before the RPI because there's a chance that MAC rotates in less than 10 minutes (which is the minimum RPI rotation period).

In the case where the MAC rotates before the RPI, we're expanding the period of time that you're advertising the identifier to the RPI rotation period instead of the MAC rotation period. However, the MAC always gets rotated again when the RPI rotates, so in practice the rotation still happens in less than 15 minutes.

In the case where the RPI rotates before the MAC, this causes the timer for MAC rotation to be reset, putting us back at the start again where either might rotate before the other.

A future Android feature request might be to allow apps to listen for MAC rotation, but this doesn't exist today. As a result, it's impossible for Android phones today to know when the MAC rotation happened, which means that it's not possible to rotate the RPI when the MAC changes! And instead, we just made sure that the RPI identifier rotates in <15 minutes, to be as "identifiable" as Android R.

WDYT, does that match with your observations?

04:36PM

Status:Accepted Won't Fix (Intended Behavior)

- **Norman Luhrmann <daughter-of-v@protonmail.com>**
  **#23Jun 18, 2020 01:11AM**

  Yes, I see your point, from Google PoV this is not a degradation of trackability.

  I would not fully agree that this is not without negative consequence in context of 3rd party BLE systems expecting an advertising start to explicitely rotate the MAC/grant anonymity though. This guarantee is no longer given until the subsequent RPI rotation happens to ensure that both MAC and RPI switch and put the device in anonymous status again.

  I do understand that this might not be in scope for the issue at hand though.

- **ap...@google.com <ap...@google.com> Jun 18, 2020 01:11AM**

- **ev...@google.com <ev...@google.com> #24Jun 18, 2020 09:50AM**

  09:50AM

  Great, thanks for your help!

I believe that 3rd party BLE systems shouldn't expect MAC rotation to imply a tracking reset, because there's no way for Android apps to know when the MAC rotation happens (this is done by the hardware, drivers or firmware, depending on the chipset).

Even though the RPI rotates the identifier in 10-15 minutes, this is not the norm for everyone that uses BLE (see https://petsymposium.org/2019/files/papers/issue3/popets-2019-0036.pdf for example). As such, I think that every protocol is ultimately the one responsible for the rotation of the identifiers, what Bluetooth Random Private Address is doing, is making sure that it doesn't introduce an additional tracking identifier, and it is pushing the privacy considerations up the stack from Bluetooth to the applications.

Anyway, this seems like a discussion for another time :-)

Is there anything else worth tracking on MITRE's side? I would love to update whoever was following along this from the outside. Please let us know if we can help.

**Norman Luhrmann <daughter-of-v@protonmail.com>**
**#25Jun 23, 2020 12:47AM**

Hi! I think you are still underestimating the ramification of ExposureNotification constantly advertising in context of Bluetooth LE devices like beacons.

You are in fact specifying subsecond advertising (though the opportunistic behavior I measured on Galaxy S10 did not reach that frequency) which is like a a signal fire for beacons to track. Pre ExposureNotification a typical beacon interaction looked like:

beacon: advertising UID/URL
mobile device: scanning every x minutes, reading UID/URL
passby number of beacon<->device interactions (moving target): very low ~ 1

An interaction with ExposureNotification active on a phone with a malicious beacon might look like:

beacon: handshake regular UID/URL interaction with device
beacon: constantly scan for ExposureNotification advertises
mobile device: run UID/URL exchange
mobile device: ExposureNotification advertising every x seconds
passby number of beacon<->device interactions (moving target): many

A ExposureNotification user is constantly advertising itself again and again to the beacons.

Due to the lack of RPI rotation during MAC rotation (I understand your remarks about driver architecture limitations) this implies that it is highly likely that as passerby handshaking a beacon will stay identifieable for the beacon over the next Bluetooth LE Smart Privacy MAC switch. This is the data correlation we were talking about initially.

Now with the timers we have on hands even if MAC is currently synchronously rotated together with the RPI, it is still highly likely that with the frequency of the ExposureNotification advertisings a beacon is able to correlate subsequent fully rotated advertisings due to the fact that the chance of multiple overlapping rotations on separate devices is negligible for small lateral clusters of devices.

Only large lateral clusters of devices would protect the user identity due to the overlap of full rotations in advertisings is larger. But even there tracking data can be post-processed (think TensorFlow feature detector) to easily handle one or more concurrent full rotations on different devices in many movement patterns. This would significantly increase device cluster size where ExposureNotification users where trackable.

Fixing the lacking rotation would improve matters a bit, but the fundamental issue remains: if a device starts ExposureNotification advertisings every few seconds it will lead to much increased communication with beacons. That might be by design, but for example - and I already brought up this topic initially - if you talked to your GDPR laywers in the meantime you might have seen that a Bluetooth LE beacon can be considered a data processor which explicitely lacks any implementation in the ExposureNotification implementations of Apple/Google.

I need you to understand the big picture. This is not a Won't Fix issue if the first app goes to a court here in Europe. I will write an agent simulation to validate my expectations, but I am certain with ExposureNotification as it is now I can do high confidence tracking of device clusters in the dozens for typical movement patterns.

We should not loose ourselves in the details of BLE driver semantics in that context. What do you think?

- **ap...@google.com <ap...@google.com> Jun 23, 2020 12:48AM**

- **ev...@google.com <ev...@google.com>** #26**Jun 23, 2020 09:09AM**

09:09AM
Hi!

To unwrap the last message a bit, here's what I understood it said, please correct me if I'm missing something:

1. Synchronizing the MAC rotation so it also triggers an RPI rotation would only improve matters a bit, and driver architecture limitations make it impossible to do it. You will write an agent simulation to confirm synchronizing it would improve matters a bit, or won't.
2. Independently of the issue around rotation, if a device starts BLE advertisements every few seconds it will lead to much increased communication with beacons, which might be by design.

Regarding (1), please let us know what you find. I think the simulation won't find a statistically significant improvement in tracking between a MAC that rotates every 10-15mins vs.

an RPI that rotates every 10-15mins vs. a MAC+RPI that rotates whenever the RPI or MAC rotate. The only thing that would change if the two identifiers were synchronized would be that the distribution of the random rotation would be significantly skewed to the left. You can easily check that by looking at the distribution of `MIN(RAND()*5+10,RAND()*5+10)` vs. `RAND()*5+10`. In fact, such skewed distribution might make tracking easier, as the likely range of random delays will not be uniform anymore, and there will be a bias (see attached graph that shows the distribution of the two-way synchronized rotation having a significant bias to the left).

Regarding (2), it does not seem to be a technical concern, but more of a legal/regulatory question that I am definitely not qualified to answer or speculate about. I am only a lawyer on TV :)

RPI, MAC and MIN(RPI,MAC).png

- **ap...@google.com <ap...@google.com> #27Jun 23, 2020 04:20PM**

  04:20PM
  ** NOTE: This is an automatically generated email **

  Hello,

  We have notified the team about this issue; they will review your report and decide whether they want to make a change or not. Thanks for letting us know.

  Regarding our Vulnerability Reward Program, the panel decided this issue's security impact does not meet the criteria to qualify for a reward in the program, so we won't be issuing a reward at this time.

Regards,
Google Security Bot

--
How did we do? Please fill out a short anonymous survey (https://goo.gl/IR3KRH).

- **Norman Luhrmann <daughter-of-v@protonmail.com>** #28**Jun 25, 2020 09:07AM**

  Please let me elaborate visually: if I use Google/Apple ExposureNotification I am close to 100% trackable. If I do not use Google/Apple ExposureNotification I am close to 0% trackable. See simulation data attached.

  The data obviously agrees that the impact of the discussed "improvements" is negligible due to the fact that your ExposureNotification turns the device in a 24/7 BLE advertiser.

  Could you explain why you adding a feature to Android (or Apple to IOS) that eliminates a core feature of BLE (namely Smart Privacy) due to a combination of BLE protocol abuse and payload structure/metadata is "intended behavior"?

- **ap...@google.com <ap...@google.com> Jun 25, 2020 09:07AM**

- **Norman Luhrmann <daughter-of-v@protonmail.com> #29Jun 25, 2020 09:13AM**

- **ev...@google.com <ev...@google.com> #30Jun 25, 2020 11:48AM**

  11:48AM
  If I understand correctly, that simulation shows that the fact that the MAC rotation does not rotate the RPI does not change the tracking. Is that correct?

- **Norman Luhrmann <daughter-of-v@protonmail.com> #31Jun 25, 2020 07:37PM**

  This is not of particular interest from my PoV. What this shows is that turning on ExposureNotification on BLE makes a device highly prone to tracking. The root problem is that ExposureNotification does constant advertising, which "normal" BLE mobile device apps do not do that way. BLE Smart Privacy will provide protection agains regular use cases of BLE profiles, but your app effectively circumvents the privacy protection by sending a constant stream of identifiers and metadata for anyone to read and store. And all that without any possibility of user consent..

- **ap...@google.com <ap...@google.com> Jun 25, 2020**

**07:37PM**

- **ev...@google.com <ev...@google.com>** #32**Jun 25, 2020 07:48PM**

  07:48PM
  Would you say that if the only thing the app did was broadcast a 0xFFFFFFFFFFFFFFFFFF it would have the same risk? (because then the attacker would just track the MAC rather than the RPI). So the risk being described is not about the contents of the advertisement, but about the fact the advertisement occurs.

- **Norman Luhrmann <daughter-of-v@protonmail.com>** #33**Jun 25, 2020 08:50PM**

  Yes I think you are right, in this context the broadcast content would be negligible as the simulation shows. The chosen (non-conventional) BLE signaling method is inherently broken from a privacy PoV.

  Any constantly advertising device would render the BLE Smart Privacy useless. But other applications use the mobile device as passive scanner, not active advertisers. Or they work in paired connections with all differences that entails. The contact tracing proximity detection via BLE does not comply with EU privacy laws from that PoV. You might also blame Bluetooth SIG

- **ap...@google.com <ap...@google.com> Jun 25, 2020 08:51PM**
- **ev...@google.com <ev...@google.com> Jul 2, 2020 06:46AM**