

Airbnb on Android just send a "Test, Test dev" push notification message
55 points by soeffemuffins23 3 hours ago | hide | past | favorite | 80 comments



add comment

Joper90 2 hours ago | next [-]

This to me means the devs have access to the prod keys, even to the external services... not good.
reply

axby 2 hours ago | parent | next [-]

How big is their dev team? Does their app change much? Could they have contracted it out and now only have one or two people who still push updates to it?
reply

Joper90 2 hours ago | root | parent | next [-]

its AirBnB, they should have this stuff sorted! Dev/prod should be completely separate with the vaults/secrets management in prod having the correct keys with only a few peeps having access (in a break glass situation). Dev's should not have the keys to put into code to push to a prod external service...
There is zero reason why any dev (or worse external dev team) should have access to prod secrets, or the ability to push out via prod. (unless someone cocked up the config for the dev/staging push notification tooling, again requires a level of access)
reply

daryiteo 2 hours ago | prev | next [-]

There is a change to Push Notification behaviour in Android 12, which all apps need to update to by November according to my team mate. So this is likely what it seems - someone made an enhancement and was testing the new behaviour on Android 12 devices.
https://developer.android.com/about/versions/12/behavior-cha...
reply

wingworks 3 hours ago | prev | next [-]

Yeep they did, I got it too. https://imgur.com/a/Yoa1G4k
reply

UIP984 3 hours ago | prev | next [-]

Same here, three minutes ago. Maybe their Key was leaked as well? I recall a similar issue happened with Firebase: https://cybernews.com/security/exposed-google-keys-leaves-bl...
reply

axby 3 hours ago | parent | next [-]

Interesting, but why would an attacker push a notification like this to so many people?
Or did not many people get it? Could I be targeted, along with the others in this thread?
If the attacker really intended to send the notification to everyone (or even 10%), wouldn't that very likely get the attention of Airbnb, and then they'd know about the issue and be able to mitigate it?
Edit: assuming everyone got it, this seemed much more likely to be a mistake, to me. For example, someone working at Airbnb was testing something and accidentally did it in prod instead of dev. Otherwise, why not camouflage this as something more innocent, like an ad for Airbnb, saying something generic like "Check out our listings near you?"
reply

SoeMyzlack 3 hours ago | root | parent | next [-]

Could be a POC for an attacker. If they got the ability to send out custom push notifications in the future they could contain malicious links.
reply

woevdbz 1 hour ago | root | parent | next [-]

If it was a poc they just lost the ability to build the real attack by being way too noticeable. This issue has likely already been mitigated and will be patched up within days if not hours. Much more likely to be an honest mistake.
reply

axby 3 hours ago | root | parent | prev | next [-]

But if so, why not try to camouflage it as something more generic, to try to avoid notifying Airbnb? I am tech savvy enough and have marketing notifications turned off, but I would assume that they are simply not honouring the setting somehow if I received an ad for Airbnb.
Now Airbnb knows to change their key or something if possible, and I'll be very suspicious of any notifications from any app in the future, especially Airbnb.
reply

999900005999 3 hours ago | root | parent | prev | next [-]

Why not just send the links. This would tip off Airbnb to patch it.
reply

axby 2 hours ago | root | parent | prev | next [-]

Oh could the attacker get information about whether or not I opened the app? Is the same key used to send notifications and access metrics that Firebase collects?
reply

alefith 1 hour ago | prev | next [-]

Everyone is blaming the process, secrets of prod etc. I'm saying, there's a test campaign problem, or, more probably, a lack of a human tester. Someone made a test in dev, it got put to the test, and wen through to prod. No real security leak or anything, just a product not properly tested. Like 99% of the internet. Who has the time and money to refactor, doc and test?
It's like climate change: let's all drive full speed into a wall, while tinkering with the stereo system of the car.
reply

StormTrooper 2 hours ago | prev | next [-]

Somewhere a junior is sweating buckets.
reply

woevdbz 2 hours ago | parent | next [-]

Maybe. But given the culture at most of these places I'd expect the junior to be explained that it's ok, everybody makes mistakes. Some engineering manager is probably sweating bigger buckets over their failure to properly secure casual human access to prod stuff, which is definitely not ok. Meanwhile the both of them are really really relieved that the notification contents were completely innocuous and not some sick inside joke that would have been massively offensive out of context.
reply

TheAceOfHearts 2 hours ago | root | parent | next [-]

The only cause for outrage would be if someone got fired for what appears to be an honest mistake.
reply

Joper90 2 hours ago | root | parent | next [-]

Unless its the CIO/CSO for shite secret management policies.
reply

Joper90 2 hours ago | parent | prev | next [-]

No, the process failed. They should NOT have access to prod API keys.. It actually shows how ABnB treats security of prod secrets.
reply

cronus94 3 hours ago | prev | next [-]

Oh thank god I was freaking out my first name is dev
reply

dgilavask 2 hours ago | prev | next [-]

Maybe they are Testing how many People will write about this on yc
reply

axby 2 hours ago | parent | next [-]

As another commenter mentioned, it's at least a good marketing campaign, causing me to open the app for the first time in months. Or it might be to gather a baseline of how many people react to their notifications, regardless of their contents? (Perhaps to immediately go to the notifications settings to disable them)
Edit: if the notification is sent by an attacker, does the attacker get access to firebase metrics as well? (Guessing they at least contain info about how many people opened the app)
reply

SoeMyzlack 3 hours ago | prev | next [-]

Just had the same notification. Can anyone else confirm this isn't some exploit being used?
reply

rickette 3 hours ago | prev | next [-]

Got it too in NL. Glad too see even the largest players make mistakes like this :)
reply

Ostendo 2 hours ago | prev | next [-]

Same here, in France. I hope the guy won't lose his job...
reply

newfoundry 2 hours ago | prev | next [-]

Got it as well. Sweden. What I noticed was that the airbnb logo was red insured if Grey in the notification. Could it be a test of changing the notification logo color?
reply

valermor 2 hours ago | prev | next [-]

Certainly some dev's fuck-up. Now it is interesting to see how they will handle it. My sympathy goes to the poor guy who made the mistake.
reply

Joper90 2 hours ago | parent | next [-]

Its the process, not the dev. A Dev should never have access to prod secrets, it show flaws in ABnB security model and tells me a fair bit around how the work with dev/deployment.
reply

newfoundry 2 hours ago | prev | next [-]

Autocorrect kills me I meant to say the airbnb logo was red in the notification instead of grey. Maybe a color change test that wasn't meant to go public?
reply

cuculetz 3 hours ago | prev | next [-]

don't know if related but when i opened it my phone rebooted with the boot logo for the os flashing (running a custom rom)
reply

SoeMyzlack 3 hours ago | parent | next [-]

Did you have developer mode enabled on your device?
reply

liikemartians 3 hours ago | prev | next [-]

Yup, I got it too in Italy. Opening the notification apparently did nothing on the surface.
reply

aftag 3 hours ago | prev | next [-]

I just got that too in the uk
reply

sanjithpk 3 hours ago | prev | next [-]

Got it too, from India
reply

otterpond 3 hours ago | prev | next [-]

got it too. made me open the app. brilliant marketing campaign
reply

axby 2 hours ago | parent | next [-]

Haha I considered this as a possibility for why it was sent... I don't ever open their app otherwise, I only ever installed it to receive messages from a host on a trip.
At the very least they might have wanted to understand a baseline for how many people will open a notification just to dig into the app and try to disable future notifications, regardless of how annoying the text in the notification was.
reply

chagalf 3 hours ago | prev | next [-]

Me too in Switzerland
reply

VictorRamayo 3 hours ago | prev | next [-]

Same here, in Mexico
reply

Alexfrance123 3 hours ago | prev | next [-]

I have it in France too
reply

Johnsteinbeck 3 hours ago | prev | next [-]

Turkey got it as well. Don't drink and work guys.
reply

Skadabucci 2 hours ago | prev | next [-]

Got it in AZ, USA
reply

shez789 2 hours ago | prev | next [-]

Just received test dev notification in Latvia.
reply

trambopoline 2 hours ago | prev | next [-]

Got it here in WA state at 12:03 PST
reply

shez789 2 hours ago | prev | next [-]

Just received this notification in Latvia.
reply

milicanogueira 1 hour ago | prev | next [-]

+ 1 Brasil
reply

Anesto 3 hours ago | prev | next [-]

Greece here, happened to me 2 minute ago
reply

wuyishan 3 hours ago | prev | next [-]

+1 from Germany
reply

Oleg11 2 hours ago | prev | next [-]

Got it as well in Brussels, BE
reply

nullified0 3 hours ago | prev | next [-]

I got this notification too. from usa
reply

patrickdavey 3 hours ago | prev | next [-]

Got it in Italy
reply

FireHalf 2 hours ago | prev | next [-]

I just received now in Turkey.
reply

Anesto 3 hours ago | prev | next [-]

Greece here, happened 2 minute ago
reply

dgilavask 2 hours ago | prev | next [-]

Only android or Apple as well?
reply

mrbombastic123 2 hours ago | prev | next [-]

Received as well in LU ;
reply

RainDropsGoBoom 3 hours ago | prev | next [-]

Recieved in Taiwan Hahaha
reply

wombatprincess 3 hours ago | prev | next [-]

Just got it, Australia
reply

Theapodig 3 hours ago | prev | next [-]

I got it in australia
reply

suddenDD 3 hours ago | prev | next [-]

Got it in Sri Lanka
reply

pockrastra 3 hours ago | prev | next [-]

Got it in Norway ffs
reply

amorsly 3 hours ago | prev | next [-]

same here in France
reply

dgilavask 3 hours ago | prev | next [-]

Got it in germany
reply

wombatprincess 3 hours ago | prev | next [-]

Got it, Australia
reply

SebastienL 3 hours ago | prev | next [-]

Got it in France
reply

Yurii7K 3 hours ago | prev | next [-]

Same here, Poland
reply

extraoriginal 2 hours ago | prev | next [-]

Got it in Italy
reply

dimitrisr 3 hours ago | prev | next [-]

Same here in GR
reply

duSky 3 hours ago | prev | next [-]

I got the same notification. australia
reply

thirumalairaj 3 hours ago | prev | next [-]

+1 from India
reply

Posterguy2 3 hours ago | prev | next [-]

+1 Australia.
reply

extraoriginal 2 hours ago | prev | next [-]

Same here
reply

mygo89 2 hours ago | prev | next [-]

Latvia +1
reply

dgilavask 3 hours ago | prev | next [-]

Got it
reply

himalayanthrust 3 hours ago | prev | next [-]

I got it too
reply

nougatmat 2 hours ago | prev | next [-]

same here DK, CPH
reply

blaziken 3 hours ago | prev | next [-]

Lol someone is getting fired!!!
reply

Joper90 2 hours ago | parent | next [-]

High up yes, not the dev who did this.
reply

dazzleivolta 2 hours ago | parent | prev | next [-]

That would actually be sad
reply

Anesto 2 hours ago | parent | prev | next [-]

Press F to pay respects
reply

nullified0 3 hours ago | prev | next [-]

got it too, from usa
reply

duSky 3 hours ago | prev | next [-]

I got this in aus
reply

hamzakhan904 3 hours ago | prev [-]

same here, pak
reply