New issue

Jump to bottom

UIAutomator2 lets anyone on the network control/view your device! #134

Closed **n0kovo** opened this issue on Dec 8, 2020 · 18 comments

Labels enhancement help wanted

n0kovo commented on Dec 8, 2020 • edited Contributor

I discovered something very concerning just now.

When using uiautomator2, which is what GramAddict is based around, it silently installs the application ATX-Agent on your device, which opens a webserver on TCP port 7912, that lets anyone on the network, with **ZERO** form of authentication, execute code, install apps, exfiltrate private data etc. on your device and view the screen remotely.

As soon as you're running GramAddict, this webserver is started. This is a ***HUGE security concern***, and should be addressed immediately!

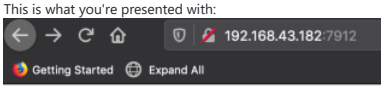
Try it yourself:

1. Find the Wi-Fi IP address of your device:
   `adb shell ip route | awk '{print $9}'`
   (NOTE: It is trivial for anyone on the same network to discover your device and the running webserver)

2. Run GramAddict as ususal.

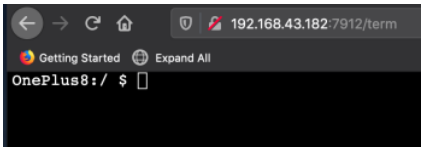
3. Using another device on the same network, go to `http://[PHONE IP]:7912` in your browser.

This is what you're presented with:

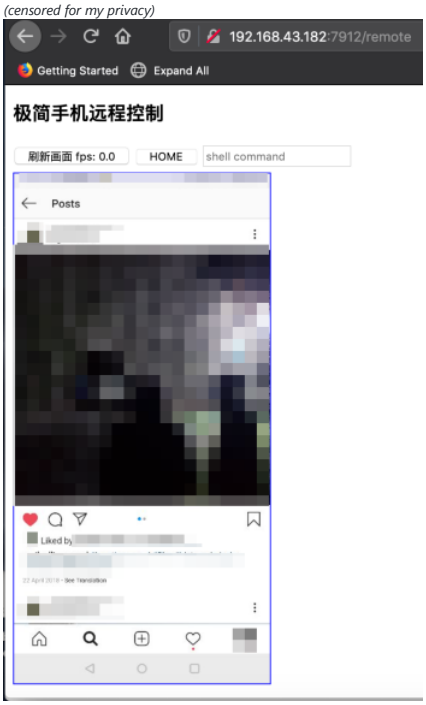


Hello ATX-Agent

- Web terminal
- API /info
- Remote view /remote



(censored for my privacy)



(Not showing the API page, as it exposes too much personal info. You can view its endpoints and capabilities at the ATX Agent page linked above)

This is extremely worrying!

philip-ulrich commented on Dec 8, 2020 Contributor

Thanks for the heads up on this. In theory this shouldn't be a problem if you are on your home network, but I do understand the concern. We are looking into this further

philip-ulrich changed the title ~~Running GramAddict lets anyone on the network control/view your device!~~ UIAutomator2 lets anyone on the network control/view your device! on Dec 8, 2020

philip-ulrich commented on Dec 8, 2020 Contributor

We've spoken internally about this. Short term we're going to add back the ability to use the stock uiautomator (which is slow and terrible) and issue a warning. This should be added back in the next release: v1.2.0.

Long term, we're going to look into forking uiautomator2 and the agent to add the ability to set a random password via ADB

👍 1

n0kovo commented on Dec 8, 2020 — Contributor, Author

Problem is, the webserver seems to keep running after quitting GramAddict. If you don't notice that and stop ATX-Agent manually, your device is fully exposed on any network you join subsequently (at least I think this is the case. I will do some more testing ASAP).

Also, you don't always have control over who is connected to your primary network. It could be guests, roommates, or of course, hackers.

As a person working with information security, I am puzzled as to why openatx wouldn't have implemented some sort of authorization. It seems insane to expose your device to the whole network. And the silent installation of ATX-Agent (or any software on the device in use, for that matter) without the user's knowledge, is super sketchy too.

👍 1

n0kovo commented on Dec 8, 2020 — Contributor, Author

Whoops, didn't see your last reply there. Sounds like a great approach. Thanks for taking this seriously.

philip-ulrich commented on Dec 8, 2020 • edited — Contributor

The agent stops automatically after a few minutes of inactivity. The readme (once you translate it) says security is something on their todo laughably.

Admittedly we didn't look into the project too much. Insomniac was already using it when we forked and it just worked really well. We have plans in place to address this quickly. Thanks for reporting - we'll keep this issue open until it's addressed.

👍 1

n0kovo commented on Dec 8, 2020 — Contributor, Author

It seems that, on my device at least, the agent keeps running for at least half an hour (haven't tested longer). Even when force killing the app, it restarts and the webserver is still listening.

philip-ulrich commented on Dec 8, 2020 — Contributor

I saw the timeout mentioned somewhere in the docs. I don't have the time to search it out again right now, but I recall it being configurable.

There are two levels of stopping the agent - one is the agent and the other is the server. If you stop both via the android app the server *should* go away. I think we can do both of those via adb and just force quit it after we finish. It gets auto restarted by the uiautomator2 framework on the next run. If we can, I'll make sure that gets added to the next update as well.

👍 1

philip-ulrich commented on Dec 13, 2020 — Contributor

So there is a lot to this issue and it's not all going to be fixed with 1.2.0. We'll keep it open for the meanwhile though.

The easy fix would be to firewall the app. The problem though is that the thing running the webserver is actually a subprocess of the minicab app and doesn't appear to show up in the non-rooted firewalls. I think this is at least partially why your killing of the processes didn't remove the server. Best way we found to kill that server is to do `adb shell pkill atx-agent` and this killed the server. This is now done after instagram is closed (which is the last action of the script before it pauses on repeat or ends). We are still evaluating ways to more properly solve this, but UIA2 is needed for now. The org behind UIA2 is aware it's a security issue, but I'll open an issue to see if we can ask them to resolve it properly. Otherwise - we'll likely have to create a fork of their code which is a whole 'nother issue.

This leads to the conversation of UIA1. UIA1 sucks - bad. Quite a lot of what we've written has been written specific to UIA2 and in general UIA2 works 100x better than UIA1. In fact, when trying to port some of the things specific to UIA2, we end up with more issues in UIA1. In trying to get UIA1 working, it also seems like instagram is able to detect it somehow and tweak their layout to make it break. It sounds fishy, but that's at least part of why #141 exists. We won't be able to likely get v1 of UIA working stable in a reasonable time so we'll likely be releasing 1.2.0 with a half-baked UIA1 implementation while we try to work out the bugs over time. Our main UIA guy has been out and I'm hitting brick walls trying to fix it.

TL;DR: We've made some progress on this, but it's not done and likely won't be done for 1.2.0.

This was referenced on Dec 13, 2020

大安全问题 openatx/atx-agent#82
Open

v1.2.0 #137
Merged

philip-ulrich added **enhancement** help wanted labels on Dec 14, 2020

n0kovo commented on Feb 2, 2021 — Contributor, Author

Any news on this?

I know it would require a huge rewrite, but if fixing openatx/uiautomator2 is not viable, maybe appium could be an alternative.

itsallmathematics commented on Feb 18, 2021

I saw the help-wanted tag on this. I'm new to GramAddict and don't know the codebase super well (nor have I programmed with UIAnimator2 before), but would be happy to help any way that I could. I mostly do software security development work & research.

👍 2

n0kovo commented on Feb 19, 2021 — Contributor, Author

@itsallmathematics Awesome! I think creating a fork of UiAutomator2 to implement some kind of authentication would be a great strategy in many ways.

👍 1

Prisscillia commented on Feb 19, 2021 • edited

@itsallmathematics **@NarkoPolo** Just a heads up I was planning on forking this repo and reading through the code base in an attempt at the same thing. Hopefully we can get this fixed together

👍 1

Prisscillia commented on Feb 19, 2021

https://vuldb.com/?id.170126

"A vulnerability was found in GramAddict up to 1.2.3. It has been rated as critical. Affected by this issue is an unknown code block of the component UIAutomator2/ATX-Agent. Impacted is confidentiality, integrity, and availability."
...
...
...

"There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product."

itsallmathematics commented on Feb 20, 2021 • edited

> **@itsallmathematics** Awesome! I think creating a fork of UiAutomator2 to implement some kind of authentication would be a great strategy in many ways.

also **@Prisscillia** , so I took a look at https://github.com/openatx/uiautomator2/search?q=atx-agent and it looks like ATX-Agent is in its own repo: https://github.com/openatx/atx-agent . It's implemented in Golang. I don't see anything auth-related in there currently. I also cannot read Chinese which seems to be the docs language. However, I used e.g. https://translate.google.com/translate?hl=en&sl=zh-CN&tl=en&u=https%3A%2F%2Fgithub.com%2Fopenatx%2Fatx-agent%2F to get a better understanding.

Yes, they mention security issues twice on there actually under "todo." So, looks like we'll need to modify UIAutomator2 to point to the forked ATX-Agent since it seems to use a hardcoded URL to retrieve it IIUC, add an auth layer for when the client connects, so GramAddict can set it as needed. Oh btw, I think vulndb picked it up because I see it has a CVE now.

philip-ulrich commented on Feb 20, 2021 — Contributor

Hello! I've had other things hit a higher level of priority in my personal so I haven't had much time to put into this aside from our quick "fix" of killing the agent when not in use.

Honestly forking and maintaining a fork of UIA2 will probably be a lot of work. If something like appium will fit our needs, then it'd prob be worth the effort to port over. We just can't go back to UIA1... it's trash.

Everything we need the library to do, is basically in the device facade file so if someone can match everything we are doing to an appium call... and appium works well.. then it could be a good move. It does seem to be a pretty active project (and not Chinese 😂) so that's a ++

philip-ulrich commented on Feb 20, 2021 — Contributor

Btw, if any of you want to become official contributors... we need some folks. 🙂 Happy to discuss further. maintainers@gramaddict.org

itsallmathematics commented on Feb 20, 2021

Some relevant info:
https://github.com/appium/appium/blob/master/docs/en/writing-running-appium/security.md
https://appium.io/docs/en/about-appium/api/

mastrolube commented on Mar 12, 2021 — Contributor

@NarkoPolo openatx/atx-agent#82 I also checked and it's fixed with v1.23.1.
Thanks **@philip-ulrich**

mastrolube closed this as completed on Mar 19, 2021

mastrolube mentioned this issue on Mar 19, 2021

dependency hotfix #183

Merged

Assignees

No one assigned

Labels

enhancement help wanted

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants