STEAM GROUP

Archi's SC Farm Archi-ASF

Outofmana Jul 22, 2021 @ 7:50am

Beware of unknown method which steal inventory through ASF IPC(on VPS)

So far two ppl on Chinese steam forum got stolen and left their inventory empty.
They both have these following features:
1. Put their ASF on VPS and IPC server on behind a reverse proxy with password.
2.There is no login record of Steam and VPS from unknown address/device.
3.ASF record shows "Global config file has been changed" then someone added them as steam friend, and they accepted automaticlly(by the "steamownerID" or "steamuserpermission" from ASF config I guess)
4.Accept all the offers from same user "The trade offer xxxxxxx is determined to be Accepted due to OtherSteamID64 76561198194377091: Master." and left inventory empty.

Is there any idea how the hacker finds their IP address/domain name of the server running ASF and password?

*Last edited by **Outofmana**; Jul 22, 2021 @ 7:51am*

A moderator of this forum has marked a post as the answer to the topic above.
Click here to jump to that post.

> *Originally posted by **Archi**:*
> I analyzed this case in our GitHub advisory:
> https://github.com/JustArchiNET/ArchiSteamFarm/security/advisories/GHSA-wxx4-66c2-vj2v
>
> Also released patched ASF version.

Showing 1-4 of 4 comments

Archi ★ Jul 23, 2021 @ 1:04am

So the user simply changed ASF config through the API and executed loot command, nothing unexpected if he managed to access the API itself.

You say that the IPCPassword was set, this is good, but it depends what it was, because if somebody set password as "asf" or something similar then the hacker could've simply guessed it right.

I'll take a deeper look if I see any way to actually skip providing IPCPassword to authorize the requests, but I doubt that this is possible. Rather I suspect misconfiguration or user's neglect.

Also, https://github.com/JustArchiNET/ArchiSteamFarm/wiki/IPC directly states that:

> Be extremely careful when you use Host values that allow remote access. Doing so will enable access to ASF's IPC interface from other machines, which may pose a security risk. We strongly recommend to use IPCPassword (and preferably your own firewall too) **at a minimum** in this case.

For example, IPCPassword will protect nothing if somebody configured his reverse-proxy to supply it automatically. Or if somebody configured ASF to trust nginx in known networks and he didn't protect his nginx against anti-bruteforce then attacker could've brute-forced the password through IP spoofing. There are a lot of factors, from what I observed majority of people do not give a single crap about security of their public ASF instances, it's easier to blame some unknown "exploit" rather than its own misconfiguration, neglecting to read the wiki and doing things right.

Of course if somebody has any proof or hint for me that ASF has a security issue which allows an attacker to skip the need of providing IPC password to every /Api endpoint, then I'll be welcome to hear it (while doing my own investigation), but for now I doubt in such possibility.

The fact that people are running insecure IPC instances is very common, I found it myself in https://github.com/JustArchiNET/ASF-ui/issues/1461 and as part of ASF V5.1.2.X I'm implementing additional measures to protect people from (their own) stupidity - but this isn't any security exploit in ASF, this is a particular misconfiguration that ASF will hopefully prevent automatically, and only a particular one too, not all possible.

It's very possible that people were not using IPCPassword at all, e.g. due to https://github.com/JustArchiNET/ASF-ui/issues/1481 issue (which is not really ASF's problem). This is also why I said multiple times that IPCPassword is the bare minimum, people using reverse-proxies to access ASF should at least have their own basic auth on top of it, which

they didn't have.

As of now, I suspect that people used ASF-ui to modify global ASF config and had their IPCPassword removed, as per ASF-ui issue #1481 linked above.

*Last edited by **Archi**; Jul 23, 2021 @ 1:25am* #1

Outofmana Jul 23, 2021 @ 1:38am

Hi,Archi thanks for your reply,I guess they've counter "https://github.com/JustArchiNET/ASF-ui/issues/1481" this issue you metioned,but they both claimed that they were using password because ASF asked for it when they logined with new device ,and they haven't changed the setting for a long time so it's weird.When they found they got stolen,IPC password has gone.

#2

Archi Jul 23, 2021 @ 1:52am

> *Originally posted by **Outofmana**:*
> Hi,Archi thanks for your reply,I guess they've counter "https://github.com/JustArchiNET/ASF-ui/issues/1481" this issue you metioned,but they both claimed that they were using password because ASF asked for it when they logined with new device ,and they haven't changed the setting for a long time so it's weird.When they found they got stolen,IPC password has gone.

They can claim anything they want to, I didn't find any way to skip a requirement of IPCPassword to access any ASF endpoint withot prior authentication, and I won't analyze specific setups to find what mistakes the user has made that lead to him getting hacked, that's what you pay security forensics for. There are a lot of possibilities what user could do wrong, some of them I listed in my post above. Until somebody presents me with a valid reproduction or proof that I'm wrong and it's possible to skip IPCPassword with proper configuration, I'll have to assume that it's user's neglect - especially considering we have linked issue that could be the root cause of that.

And this is on top of the fact that user didn't set up ANY additional security as ASF wiki strongly recommended when exposing IPC to the public. Even nginx basic auth would've stopped that.

*Last edited by **Archi**; Jul 23, 2021 @ 1:56am* #3

A moderator of this forum has indicated that this post answers the original topic.

Archi Jul 23, 2021 @ 9:39am

I analyzed this case in our GitHub advisory:
https://github.com/JustArchiNET/ArchiSteamFarm/security/advisories/GHSA-wxx4-66c2-vj2v

Also released patched ASF version.

#4

Showing 1-4 of 4 comments

Per page: 15 30 50