



SECURITY
RESEARCH

LAST MESSAGE TO CANAL+ CSO

This document contains a copy of the last message sent on Aug 30, 2022 through LinkedIn platform to CANAL+ CSO. The message was a result of a failed attempt to reach out to multiple personnel at CANAL+ France and Poland (CEO, VP of Technology, CTO, PR and security persons).

Dear Mrs. XXXXXX XXXXX,

Let me express some thoughts before our LinkedIn contact gets lost...

I need to say that I find the following kind of weird:

- the only contact to Canal+ is through LinkedIn, I don't know if this can be treated as an official (not to mention secure) comm channel, not sure about the reasons why you stick to that channel instead of the usual (the case for most big companies I have been dealing with), more secure (PGP encrypted) and more official e-mail contact, sorry to say that, but to me it looks as if your company was not willing to have the contact at all

- I haven't heard from anyone else from Canal+ (France or Poland) even though I have reached out to many people through e-mail and SMS...

- you expressed no need to have the actual technical details to be provided to your end, this either means that you got these from Microsoft (them handing over my research to you) or you believe that you got complete understanding of the issue (got all the info) from the movies. IMHO you are making your own work more difficulty as you are missing details not present in the movies that could help you understand how to improve STB / content security, what secrets need to be changed, what APIs tightened, what changes at CDN / watermarking should be done, etc.



SECURITY
RESEARCH

- the only information I have from your end is that you will work on the issues (not sure if you are to fix anything).

I haven't decided about the disclosure, but if that is to happen I'd like to coordinate it with your end, would like to know what issues got fixed (if any got fixed), whether these were indeed attributed to your end (MS response indicates this is not the problem with their license server, I'd like to know if that is indeed true).

I'd like to know if STBs are to be updated, if you are willing to provide any credits at that time to my end (on your web pages, in the upgrade note displayed on TVs describing upgrade content, etc.).

I personally think it is better to coordinate stuff / cooperate on the topic instead of the usual "we don't work with this guy" approach taken by the industry.

Please, take into account that it has been a 3rd time I was able to show inadequate content security of the platform Canal+ is now the owner of. There has been issues affecting end users too, which look exploitable 3 years following the disclosure and which I would like to have fixed in particular.

That said, instead of have you caught by surprise when the research gets released by my end some time in the future (you might find out that you missed something / didn't fix everything, etc.) and for the reasons outlined above, I would like to ask you to consider the establishing of a more official contact with my end.

Thank you.

Best Regards,

adam