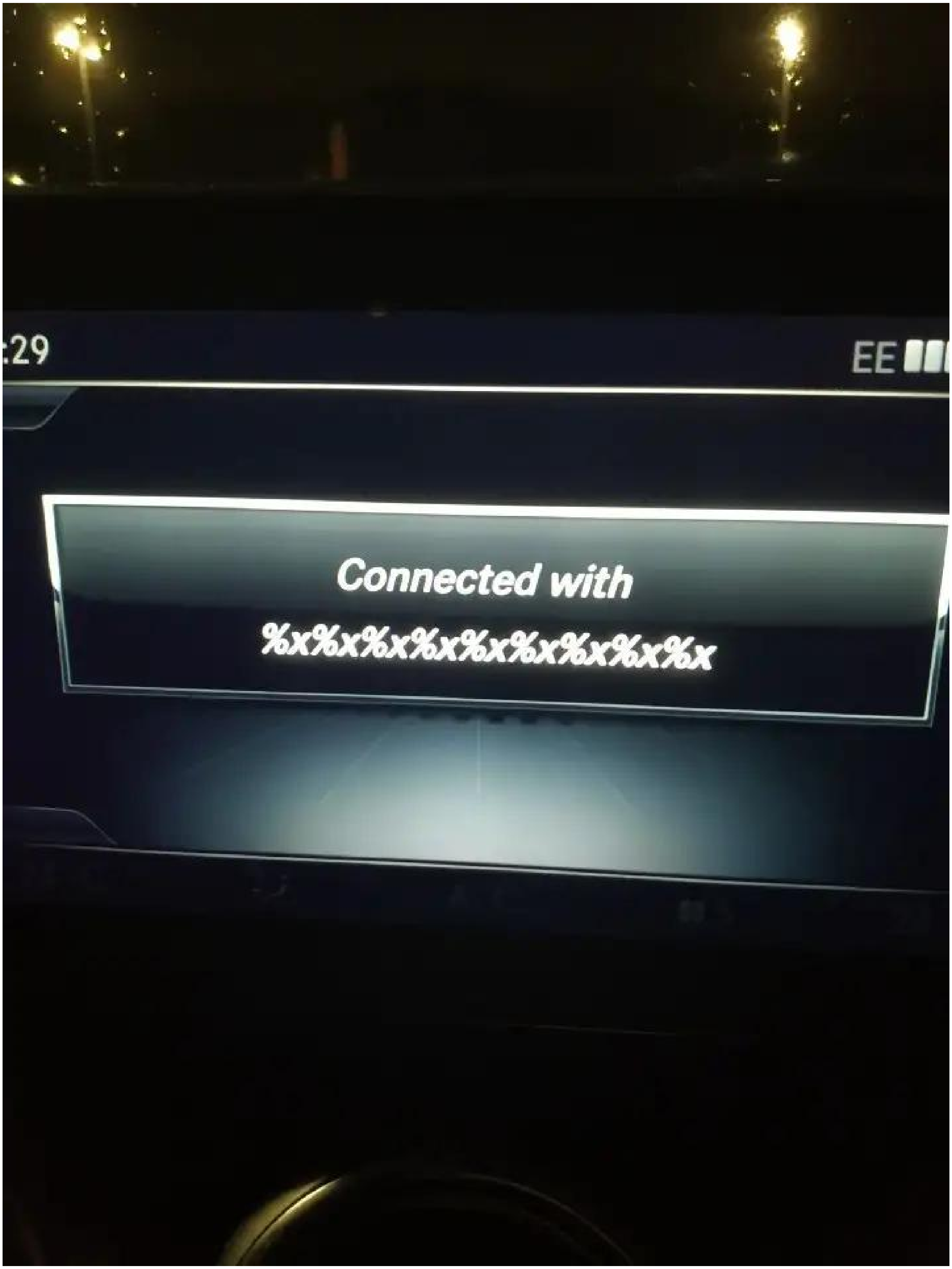
Liam B Follow
Aug 24, 2020 · 2 min read · Listen

Mercedes COMAND Infotainment improper format strings handling

I fairly recently attended some training regarding pulling information from PCBs among other things revolving around potential attacks focusing on operational technology. Toward the end of the training, other attacks in the real world were discussed with a number of examples shown. One of the examples was that of the following tweet.

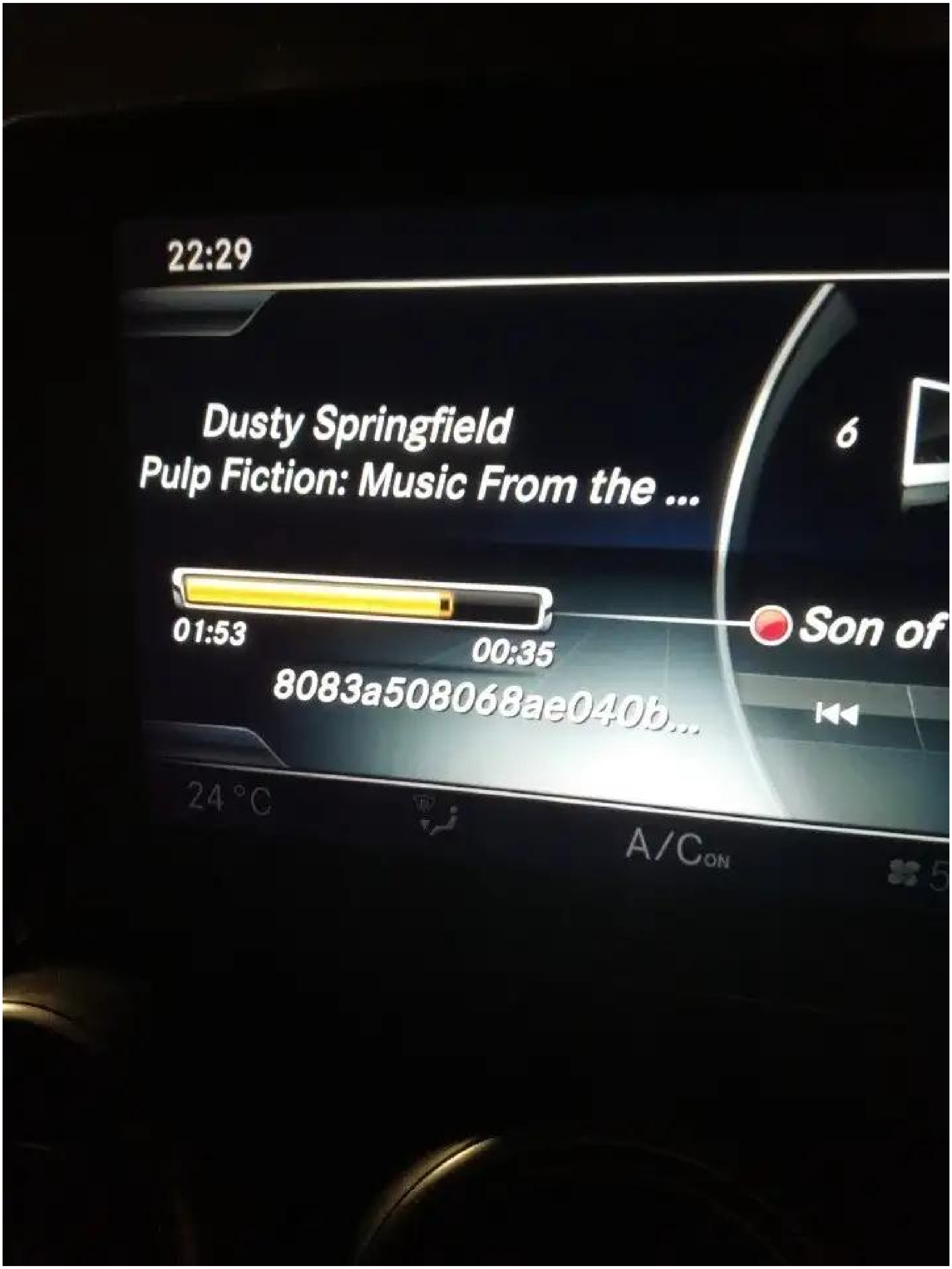
I was curious to see if this would work on my own car, as over time I'd changed my phone name in hopes that something would pop somewhere along the many random devices I connect to on a weekly basis. (I don't really).

After getting back from Spain, I returned to my car with the knowledge of some strings that may work thanks to the above tweet. So I instantly set my phone's bluetooth name to "%x%x%x%x%x%x%x%x%x%x" before starting my car in an excitement.



Connected with

%x%x%x%x%x%x%x%x%x



Once that had confirmed to have worked. I kind of left it at that. Reading through the Twitter thread earlier, I had seen numerous people who had the same issue and had ended up bricking their infotainment system. This car is my daily driver so I didn't want to brick the infotainment system and have to take it into Mercedes for them to charge me an arm and leg to fix the issue.

I did report this to Mercedes through their vulnerability disclosure program but was informed it isn't an issue. So essentially I wanted to disclose it here so people could research it further and see if they can find something a bit more juicy, even if it is just a bricking of the infotainment system, at least then I'd have something a bit more juicy to go back to Mercedes with.

Timeline of disclosure

13th December 2019 — Reported to Mercedes through their vulnerability disclosure

19th December 2019 — First response from Mercedes

24th January 2020 — Confirmation that this is felt to not be an issue

10th March 2020 — I reference the above tweet and ask if Mercedes mind me posting about issue for people to research.

11th March 2020 — Mercedes ask if I can await them to make a decision about this

27th August 2020 — Assigned CVE-2020–16142

So after waiting for a while. I've posted it. If anyone does have any further joy, I would greatly appreciate any information about how you've done it and what you've achieved.