KOFFEE
Kia OFFensivE Exploit

G. Costantino
I. Matteucci

ISTITUTO di INFORMATICA e TELEMATICA

Consiglio Nazionale delle Ricerche

Automotive attacks

Remote Exploitation of an Unaltered Passenger Vehicle.
C.Miller and C. Valasek, BlackHat 2015

TBONE – A zero-click exploit for Tesla MCUs
R. Weinmann and B. Schmotzle

2014

2018

2020

2021

0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars
BlackHat 2019

KIA Ceed

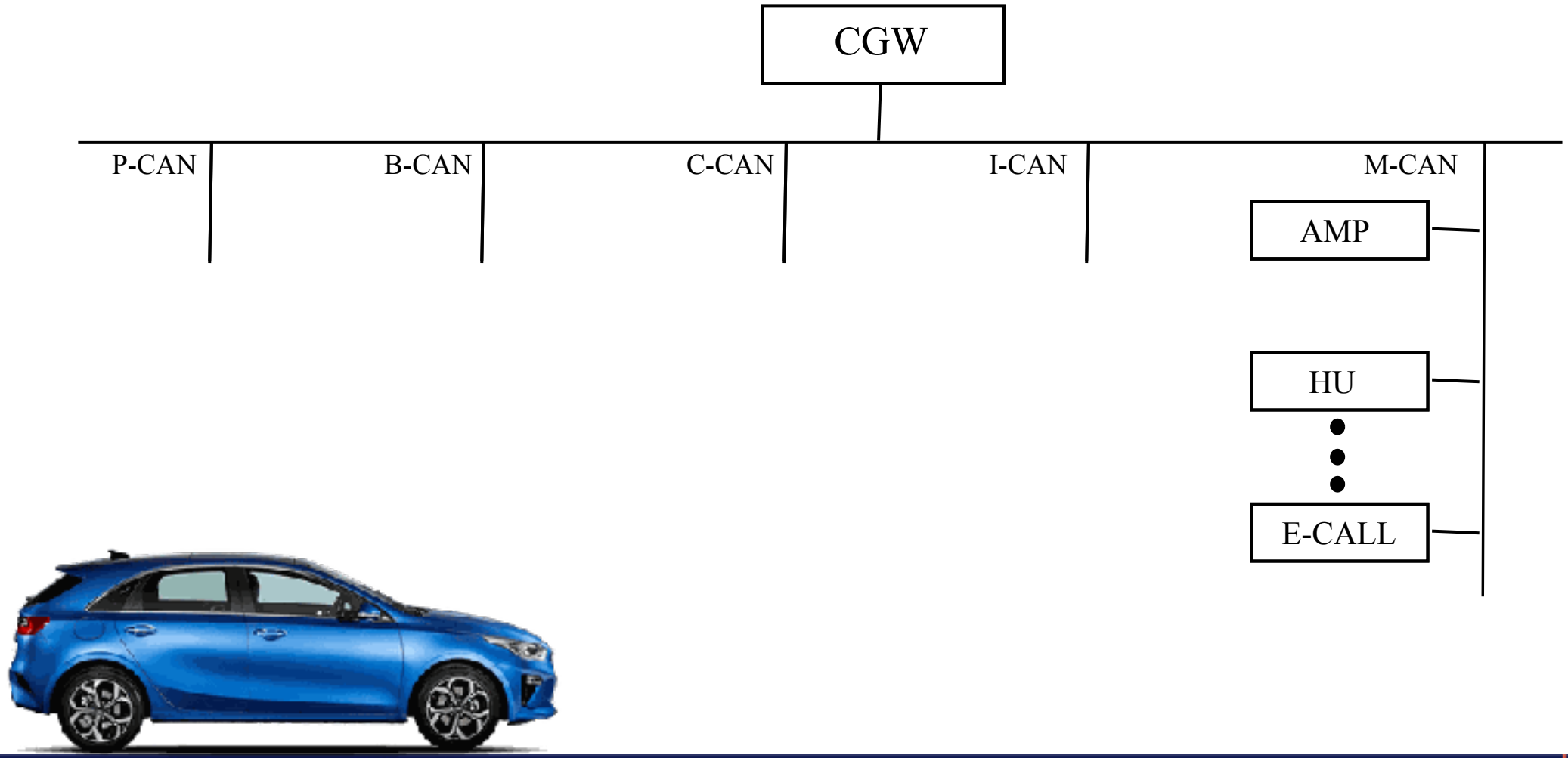
07/2019 — **2020** — **03/2021** — **2021 ?**

Paper with full details

KIA Ceed \ Why?

- Head Unit (HU) with Android OS
- Connection to the Internet (via Hotspot or 4G/5G modem)
- Installation of third-party APPs (not officially)
- HU connected to the CAN bus?
  - *We did not know…*

KIA Ceed \ In-vehicle anatomy

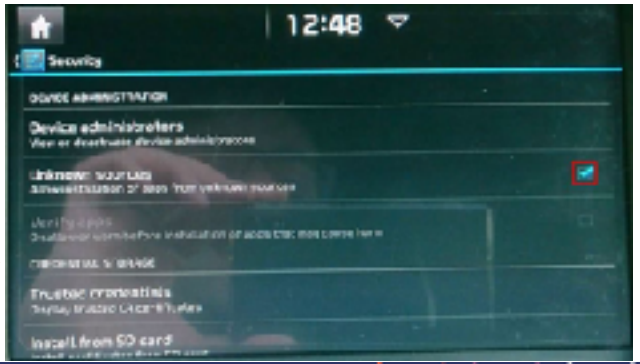


KIA Ceed \ Head Unit

- Gen 5.0, referred with the name *iAVN*
- Android OS version 4.2.2
- CPU ARM Cortex A9 @ 1.2 to 1.5 GHz
- Display 8" touch-screen
- Wi-Fi and bluetooth

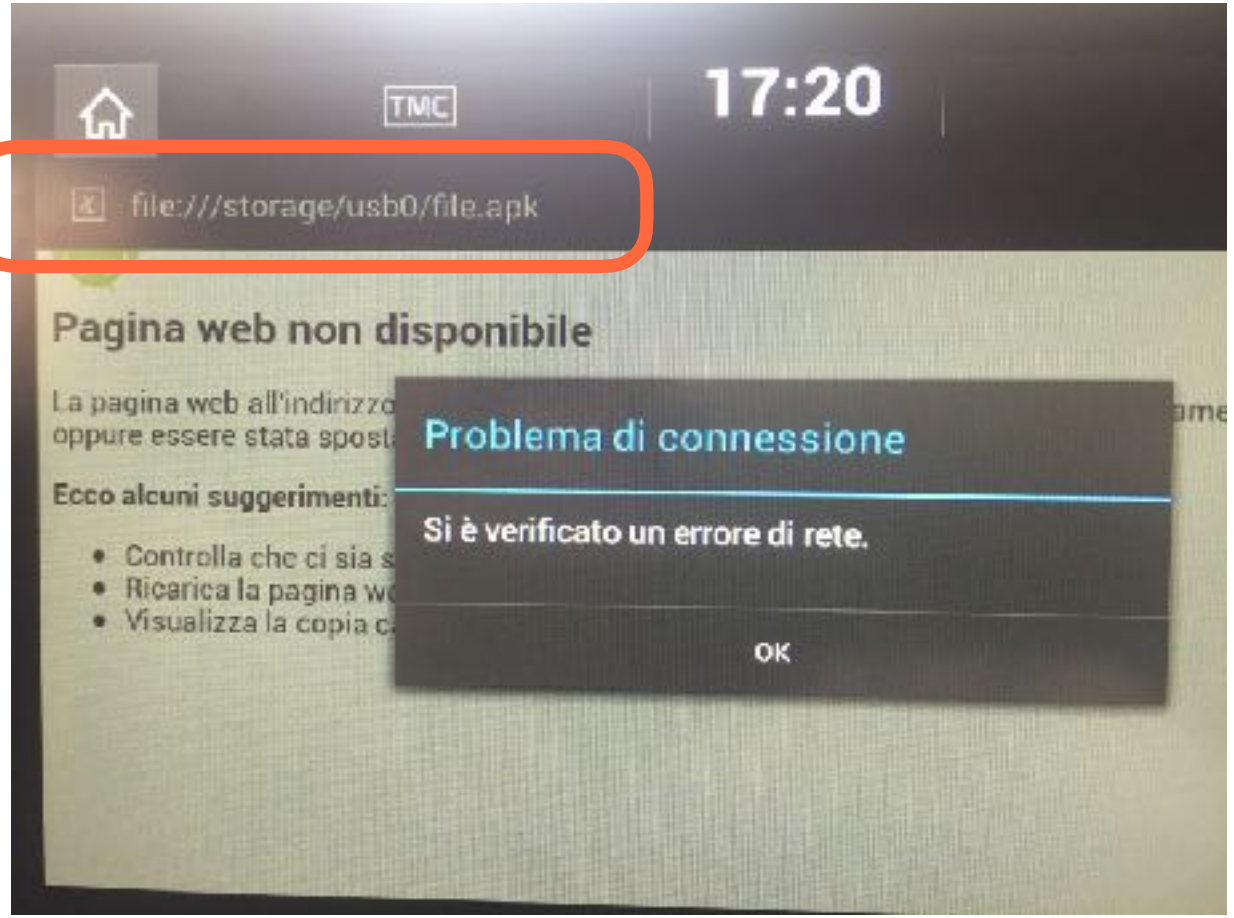
KIA Ceed \ Head Unit \ Engineering menu

- Full access to the HU through the end menu
- Accessing to all installed apps
  - System apps
  - User apps
- Installing third-party app



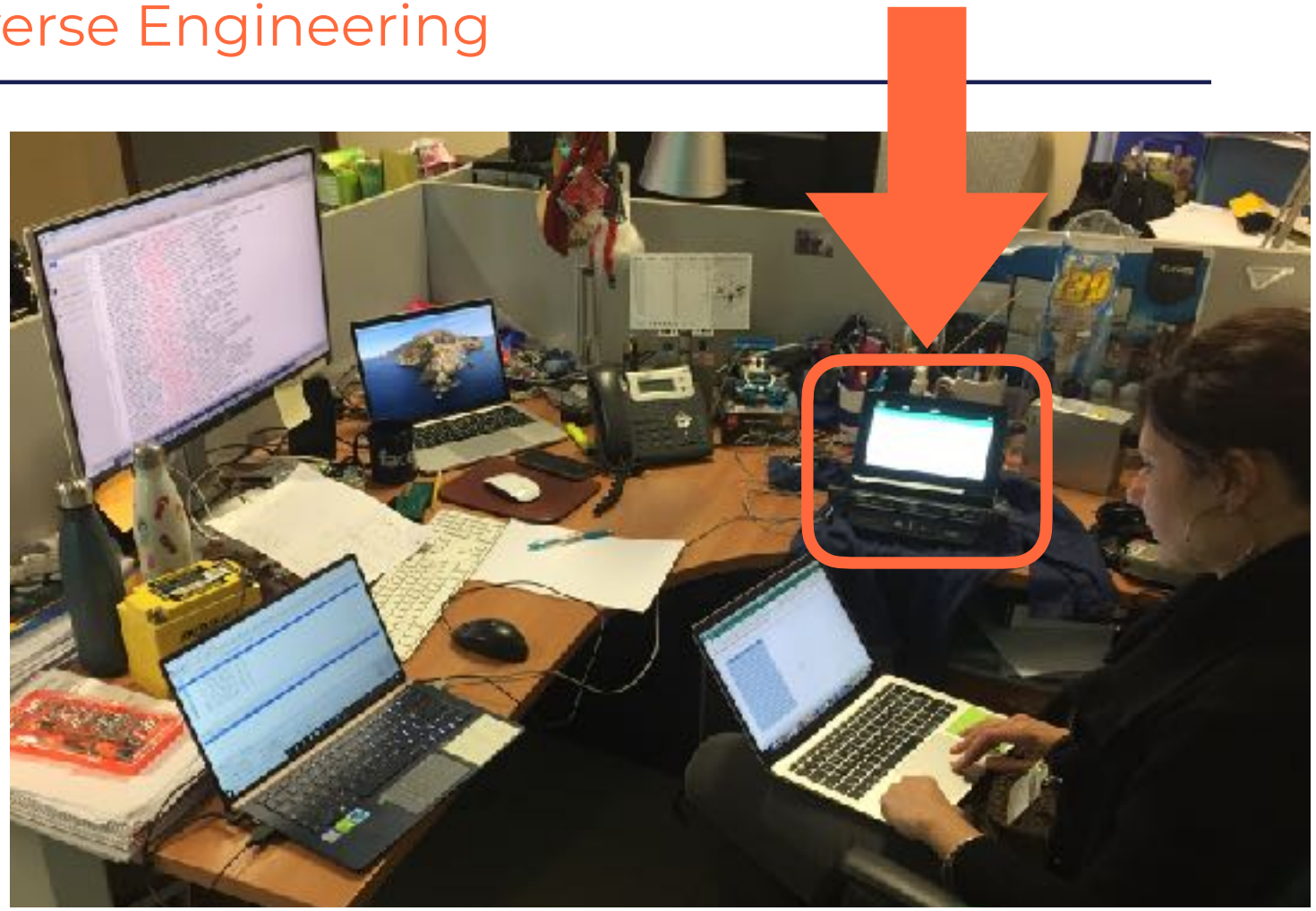
KIA Ceed \ Head Unit \ Engineering menu \ Third-party app

- We can use the browser (system app) to install android apps (app):
  - From usb
  - From remote server



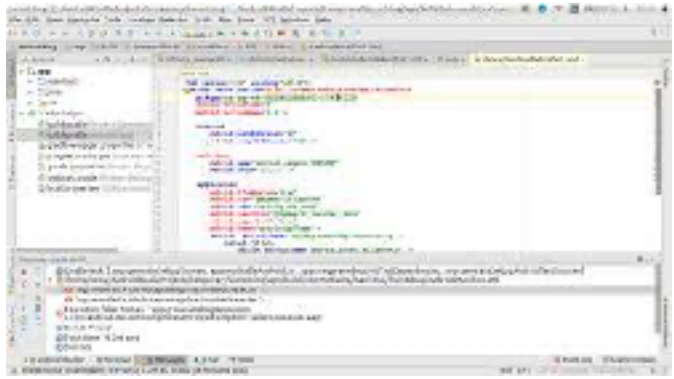
KIA Ceed \ Head Unit \ Reverse Engineering

- HU in the lab
- Starting reverse eng:
  - File system
  - All HU apps
- SOP.003.30.18.0703
  - 98 apps
  - 2.654.557 source code lines (java + xml)
  -



KIA Ceed \ Head Unit \ Reverse Engineering

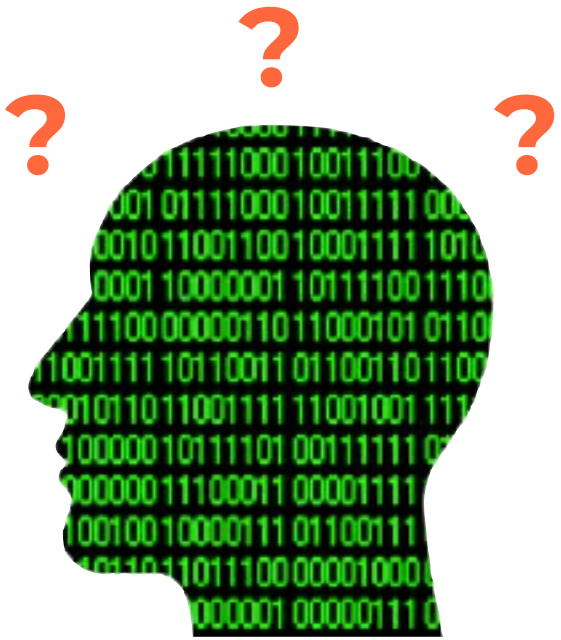
APK + ODEX



Source Code

Goal

- Any line of code that shows how to control the HU and/or sends CAN bus frames



KIA Ceed \ Head Unit \ Reverse Engineering \ Decompilation process

Fuzzy search

```
private boolean sendMicomMsg(String msg) {
    try {
        Process process = Runtime.getRuntime().exec("micomd -c inject " + msg);
        process.getErrorStream().close();
        process.getInputStream().close();
        process.getOutputStream().close();
        process.waitFor();
        Thread.sleep(1);
        return true;
    } catch (Exception e) {
        e.printStackTrace();
        Log.e(AutoTestService.LOG_AUTO_TOOL, "Micom command error (sendMicomMsg)!");
        return false;
    }
}
```

KIA Ceed \ Head Unit \ Reverse Engineering \ local attack \ micomd

Goal

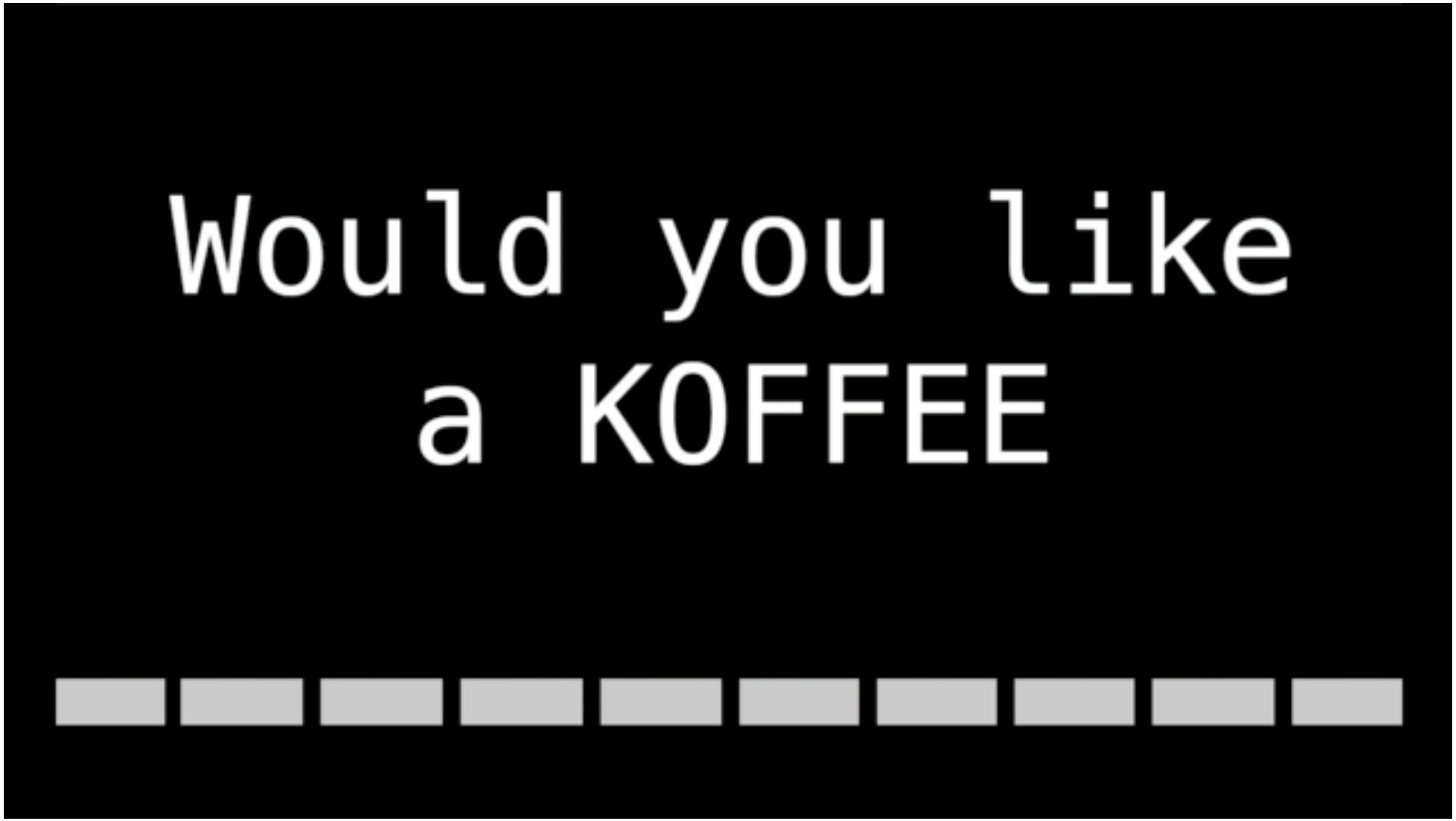
- Locally injecting micom message to activate HU functionalities and sending CAN bus frames into M-bus

KOFFEE \ Exploit \ End2End attack

Goal

- Remotely Injecting micom message to activate HU functionalities and sending CAN bus frames into M-bus

KOFFEE \ Head Unit \ Reverse Engineering \ demo



KOFFEE \ CVE

Printer-Friendly View

CVE-ID	
CVE-2020-8539	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Kia Motors Head Unit with Software version: SOP.003.30.18.0703, SOP.005.7.181019, and SOP.007.1.191209 may allow an attacker to inject unauthorized commands, by executing the micomd executable deamon, to trigger unintended functionalities. In addition, this executable may be used by an attacker to inject commands to generate CAN frames that are sent into the M-CAN bus (Multimedia CAN bus) of the vehicle.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://gist.github.com/gianpyc/4dc8b0d0c29774a10a97785711e325c3
- MISC:https://sowhat.iit.cnr.it/pdf/IIT-20-2020.pdf

Assigning CNA

MITRE Corporation

Date Record Created

20200203	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

KOFFEE \ Exploit

RAPID7 Metasploit

04/2021

KOFFEE Exploit

Vulnerable Head Unit software versions

- SOP.003.30.180703
- SOP.005.7.181019
- SOP.007.1.191209

Verification Steps

- [ ] Start `msfconsole`
- [ ] `use post/android/local/koffee`
- [ ] `set session 1`
- [ ] `toogle_radio_mute` or `run`

Actions

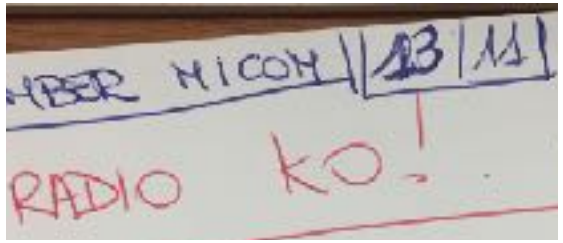
- CAMERA_REVERSE_OFF: It hides the parking camera video stream
- CAMERA_REVERSE_ON: It shows the parking camera video stream
- CLUSTER_CHANGE_LANGUAGE: It changes the cluster language
- CLUSTER_RADIO_INFO: It shows radio info in the instrument cluster
- SET_NAVIGATION_ADDRESS: It pops up the navigation address window
- SWITCH_OFF_Hu: It switches off the head unit
- SWITCH_ON_Hu: It switches on the head unit
- TOGGLE_RADIO_MUTE It mutes/unmutes the radio

Timeline \ Responsible Disclosure

07/2019

KIA
Ceed@CNR

13/11/2019



02/2020

KOFFEE

04/2020

09/2020

Updated
HU software

11/2020

Technical
paper

12/2020

CVE

04/2021

Full paper
submitted

Thank you!