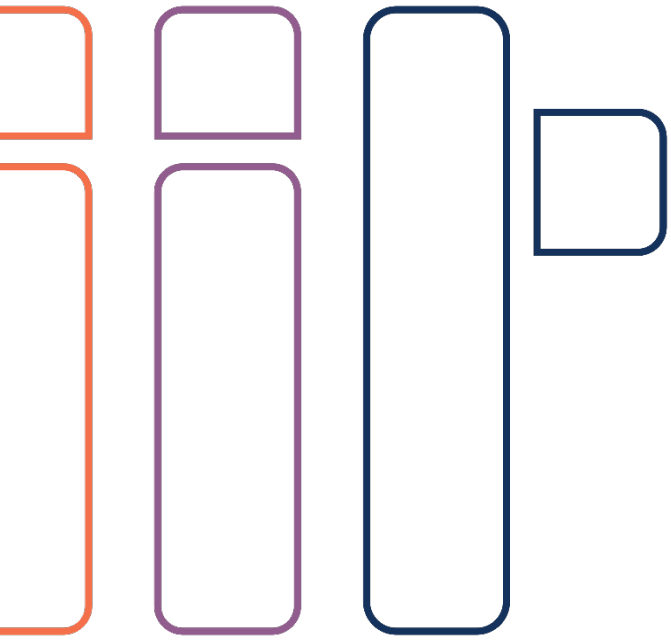

TECHNICAL REPORT

IIT TR-01/2023

CHIMAERA - Custom Hyundai Motor group infotAinmEnt fiRmwAre

G. Costantino, M. De Vincenzi, I. Matteucci

ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche

CHIMAERA

Custom **H**yundai **M**otor group infot**A**inm**E**nt fi**R**mw**A**re

Gianpiero Costantino, Marco De Vincenzi, Ilaria Matteucci
Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche
e-mail: firstname.lastname@iit.cnr.it

Revision History

Revision	Date	Author(s)	Description
1.0	09.11.2022	CNR	First Version.
1.1	19.12.2022	CNR	Added implementation and proof details.
1.2	22.12.2022	CNR	Minor updates plus editing after Hyundai review.
1.3	29.12.2022	CNR	Minor updates plus editing after Hyundai review.
1.4	12.01.2023	CNR	Final version after Hyundai review.

1 Introduction

At the beginning of 2022, we started a vulnerability assessment of the In-Vehicle Infotainment (IVI) system *Gen5W_L* [1] firmware which is part of Hyundai, Kia, and Genesis vehicles. In October 2022, as result, we have found different issues, like a memory leak vulnerability, that allow us to create our customized firmware. This study is part of one of our research activities to identify vulnerabilities in complex computer systems and publish the achieved results following the responsible disclosure process. Thus, in November 2022 we have started with Hyundai Motor Group the responsible disclosure process.

Leveraging the experience got with the Gen5 ([CVE-2020-8539][2] and *KOFFEE* - Kia OFFensivE[3] exploit), we analyzed a Gen5W firmware and we were able to find several security issues. The main finding is the possibility to leak data from the memory during the decryption process and, consequently, we can retrieve the AES-CBC 128 key, the initialization vectors, the method to generate the SHA 256 of each file, and bypass the check of the digital signature. We also identify the specific structure of the firmware files, which is necessary to modify them.

In the following Figure 1, we show the working weeks with the different phases and the relative activities and findings. The diameters of the circles represent the effort spent for each phase and in bold we report the main activity for each phase.

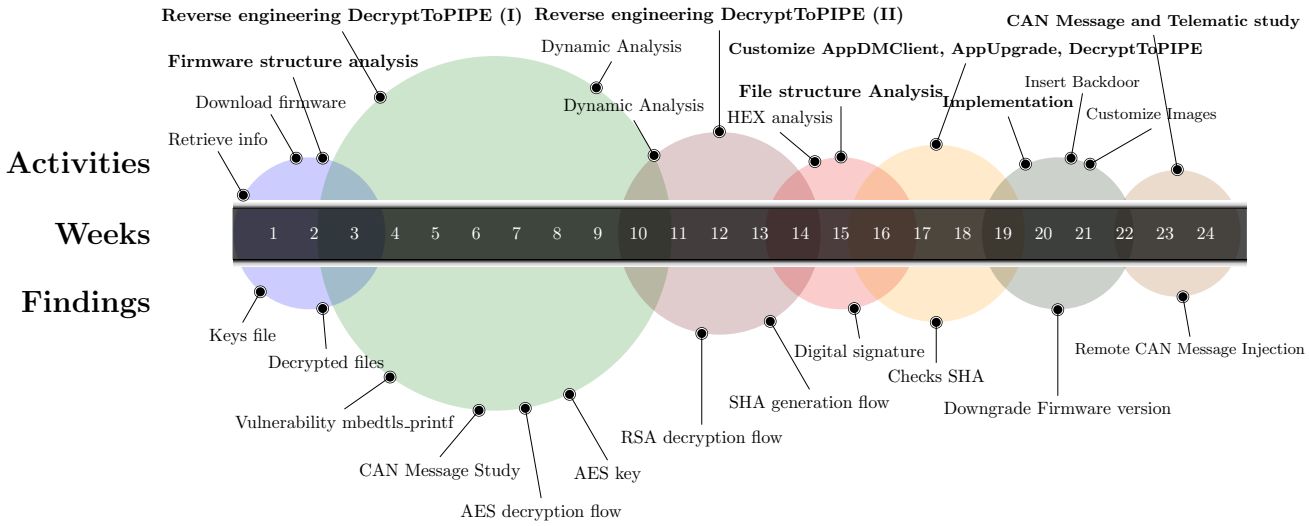

Figure 1: The timeline shows the activities, findings, and effort. In bold is reported the main activity for each phase.

2 Research Findings

The security issues that we found allow us to replay the firmware encryption operations, install our custom firmware on the LGE infotainment system, create a backdoor to remotely control the Gen5w units and inject CAN bus frames.

In the following, we list our findings:

[1] *Gen5W_L* represents the state of art of HU sold in Hyundai Motor Group vehicles with In-Vehicle Infotainment systems based on Linux

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8539

[3] https://sowhat.iit.cnr.it:8443/can-work/koffee

- Compute and read the encrypted AES-CBC 128 key;
- Extract the RSA public key;
- Decode the AES-CBC 128 key using the previous RSA public key;
- Compute the SHA256 of the content of each file;
- Discover the algorithm that generates the Initialization Vector (IV) for the AES-CBC cryptosystem;
- Generate the Initialization Vector (IV);
- Encode and decode each file with the AES-CBC 128 Key and the IV;
- Bypass the check of the digital signature during the firmware installation by upgrading AppDMClient binary patch in Head-Unit;
- Remotely control the Gen5W IVI system by injecting remote commands that impact also the CAN bus into M-bus, B-bus and C-bus. In particular, we forge CAN bus frames like we trigger services from the telematic app, e.g., Bluelink. This is possible only leveraging 1-Day exploit (AppNavi - see Section 5) or using our custom firmware.

To conclude, with our discoveries, we can almost customize any part of the firmware, so, in our implementation, we modify the firmware version number and date, some images, and we insert a backdoor. Note that the custom firmware can be installed on Head-Unit in which is installed old version firmware (prior to March 2022) operable 1-Day exploit (AppNavi - see Section 5). Currently, as far as we know there are no known 0-Day vulnerabilities that can be available in the Head-Unit of the latest version firmware. Hyundai HQ is aware of the AppNavi vulnerability. It was deploy on March 2022, but it was eliminated in the latest firmware version. Nevertheless, we know how to downgrade the Head-Unit firmware from last available version, i.e., 221129, to a version prior to March 2022 that can be exploited using the AppNavi vulnerability, which is not present in the last firmware version.

3 PROOF

A proof of our work can be done through the customization, and the subsequent encryption of a firmware file. So, we perform an arbitrary change of version number written within the *.lge.upgrade.xml* file, which is possible only with a custom firmware. We create a new *.lge.upgrade.xml* where the version number is AE_E_PE.EUR.CHIMAERA_CF01.808489, we encrypt and test it on an Gen5_L, LGE based infotainment system. In Figure 2, we show how the system reads and accepts the new version, just before installing it. We started the installation upgrade and the custom firmware worked as expected.

Besides, during the firmware customization, we modify the following images:

- The home background as reported in Figure 3;
- The numbers of the radio stations as reported in Figure 4;
- We modify two button icon images. We substitute the original settings buttons with two customized icon images as reported in Figure 3;
- We modify the image of a chip in the setting menu as reported in Figure 6;

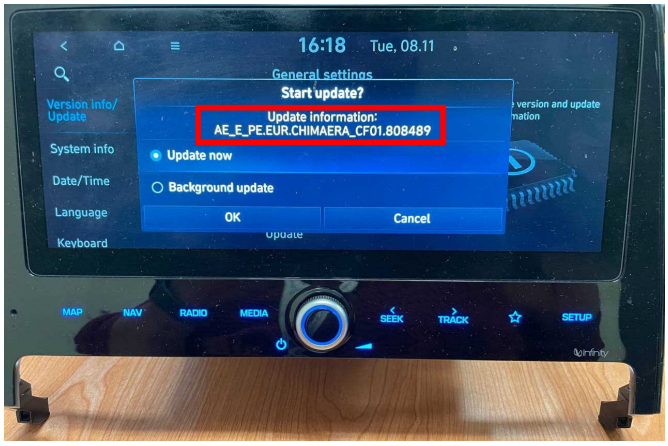

Figure 2: Ioniq IVI system (LGE based) with the new version number read during the upgrade.

Figure 3: Our customize home background.

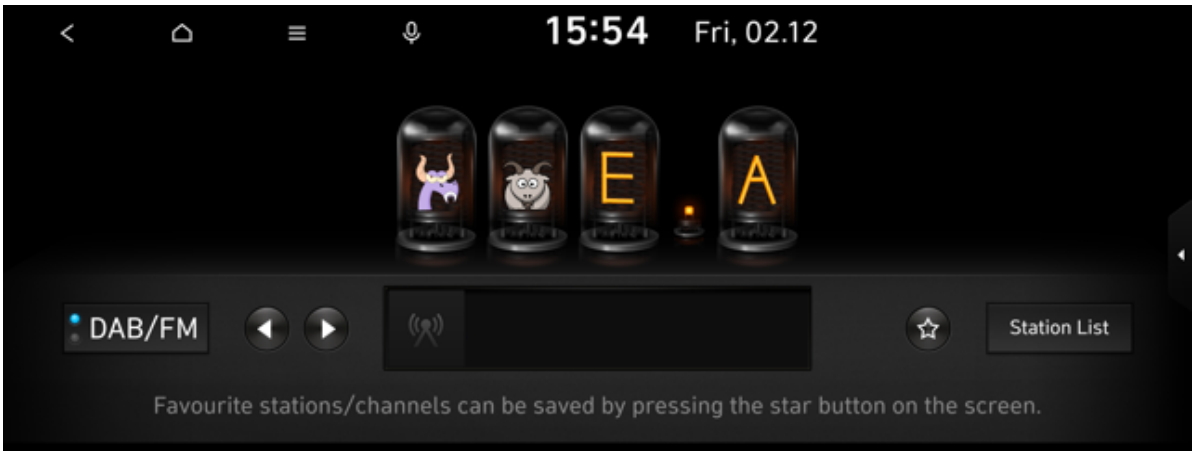

Figure 4: Our customize radio station search. Instead of the numbers in the bulbs, we show the letters of Chimaera and our icons.

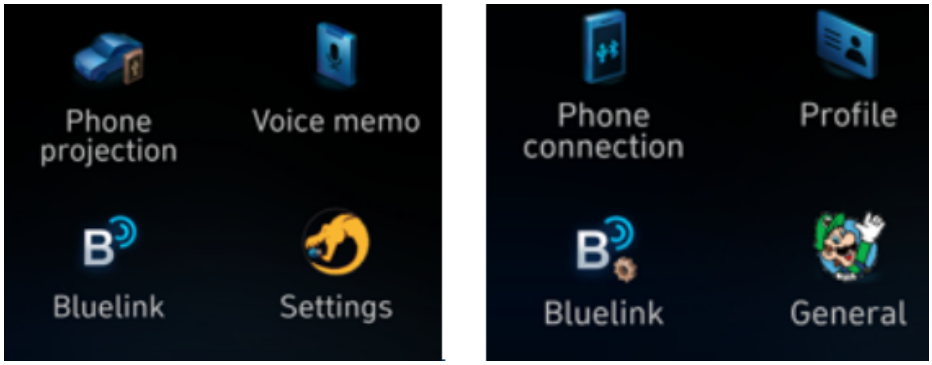

Figure 5: Customized “Settings” button in the left image, and the “General” button in the right image.

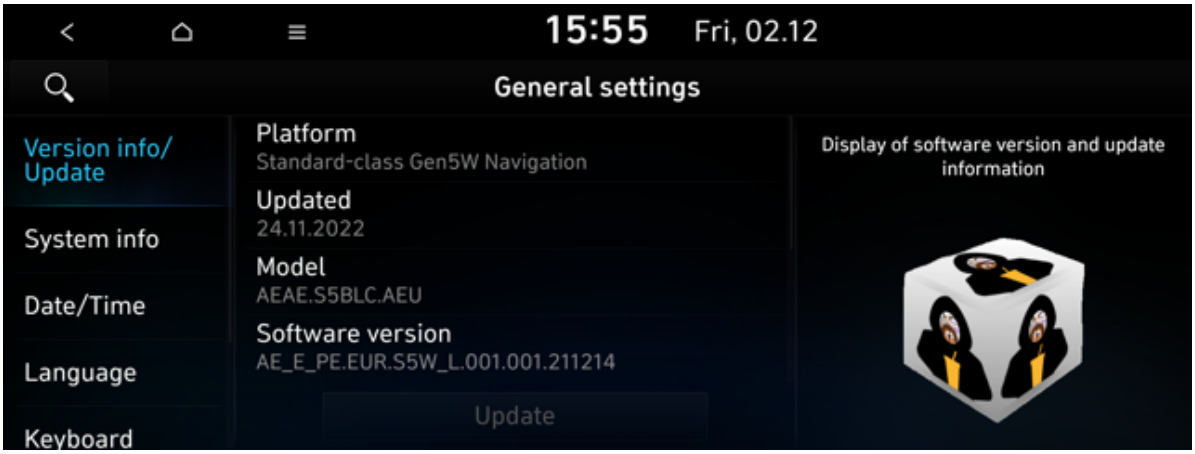

Figure 6: Customized image in the setting menu.

3.1 Custom Firmware Proof - latest version

We were able to create a custom firmware by installing a customized version of last available firmware in which we inserted only a backdoor for remote access. The head unit employed to test this last version is of a Kia Niro MY20. In Figure 7 we show the “cat” command that displays the version number. Instead, in Figure 8, we show the screenshot taken from the head unit in which the setting window shows the version number of the installed software.

```
root@prm-gen-5:/etc# cat version.txt
5W.XXX.S5W_L.001.001.221129
```

Figure 7: Cat command executed on the last version.

4 Responsible Disclosure

As Italian National Research Council, we aim to publish our findings and results, so this report can be considered as the start process of the responsible disclosure with the Hyundai Motor Group, which started on November 9, 2022. Full details of our work will be given after the end of the responsible disclosure process.

Figure 8: Settings windows screenshot.

5 Acknowledgment

We thank the open-source project [4] on GitLab that shows how ot exploit the AppNavi vulnerability.

[4] https://gitlab.com/g4933/