SECURITY ADVISORY

Vulnerabilities in Skoda and Volkswagen vehicles

Vulnerabilities in Skoda cloud backend

2023.11.22

PRODUCT DESCRIPTION

Vulnerabilities affecting Skoda and Volkswagen Group vehicles were originally identified in Skoda Superb III (3V3) - 2.0 TDI manufactured in 2022.

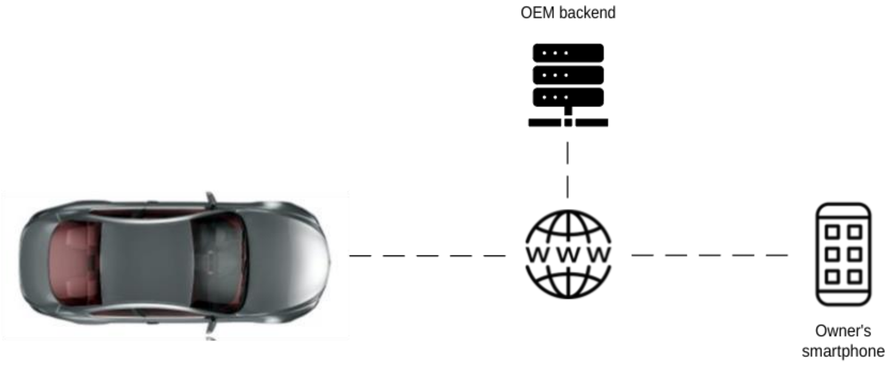
Skoda Superb is a D-segment (mid-size/large) family car designed and produced by the Czech car manufacturer Skoda Auto since 2001. The third generation that is currently in production uses the MQB platform. Skoda Superb III entered production in 2015.

Skoda Superb III 2022 (image source: skoda.hu)

The car has the following features:

- MIB3 infotainment unit with touch-screen display – the unit manufactured by Preh and used in Skoda and Volkswagen cars
- SmartLink function that enables the car to communicate with owner’s portable devices via Android Auto, Apple CarPlay, MirrorLink, and potentially other communication technologies
- TCU with emergency call (E-call) function implemented via cellular network

The car uses TCU and cellular communication channel to stay online, receive OTA updates, and communicate with OEM backend.



Communication scheme between vehicle and owner’s portable device

To communicate with their cars, owners can use MySKODA application available for Android and iOS.

The newest version of the MyŠKODA app is now available to download.

12:30

ACTIVATED

ENYAQ iV

Doors and lights

Vehicle Locked

Parking Lights Off

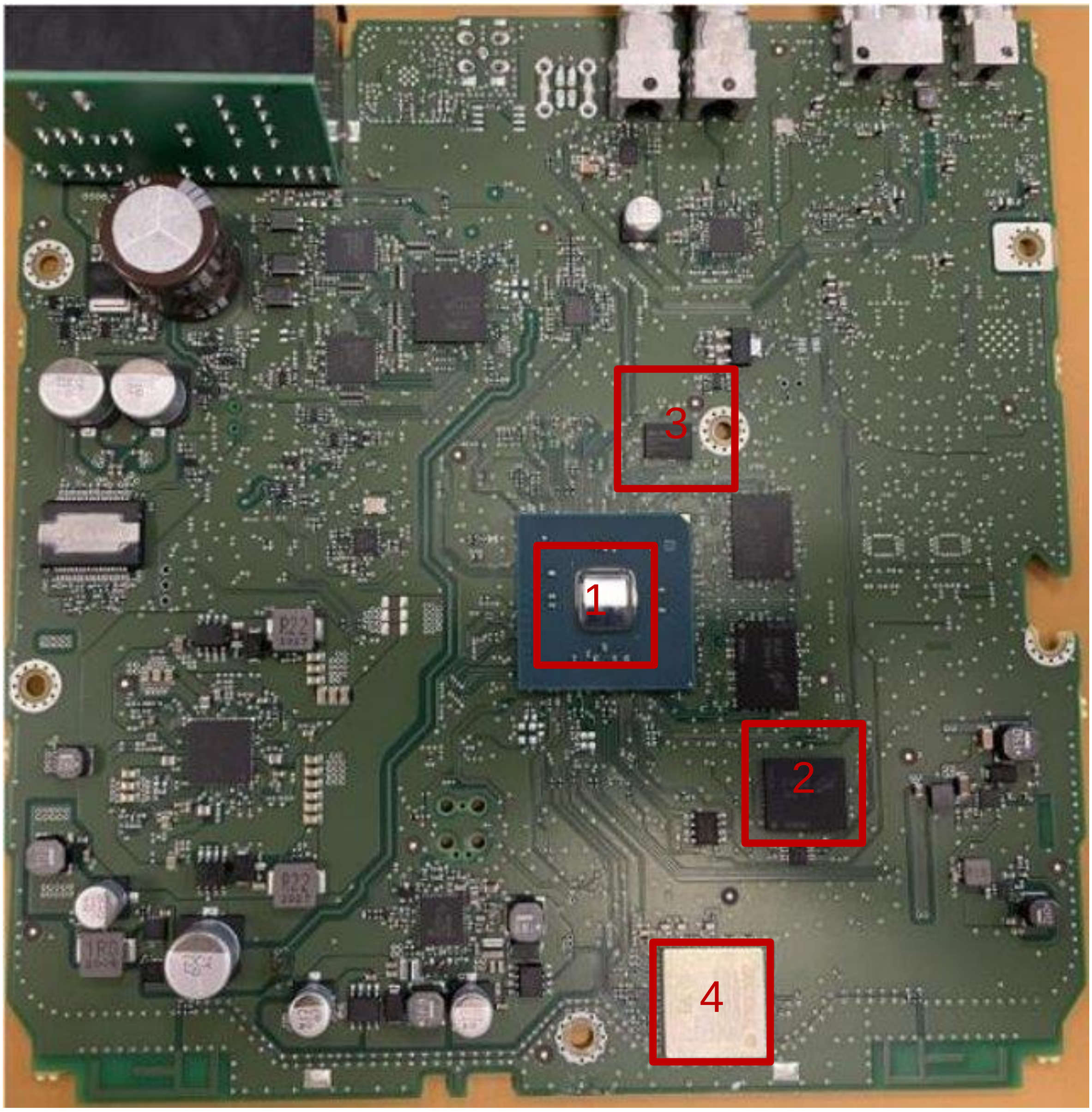
Doors / Windows Open

Battery charging

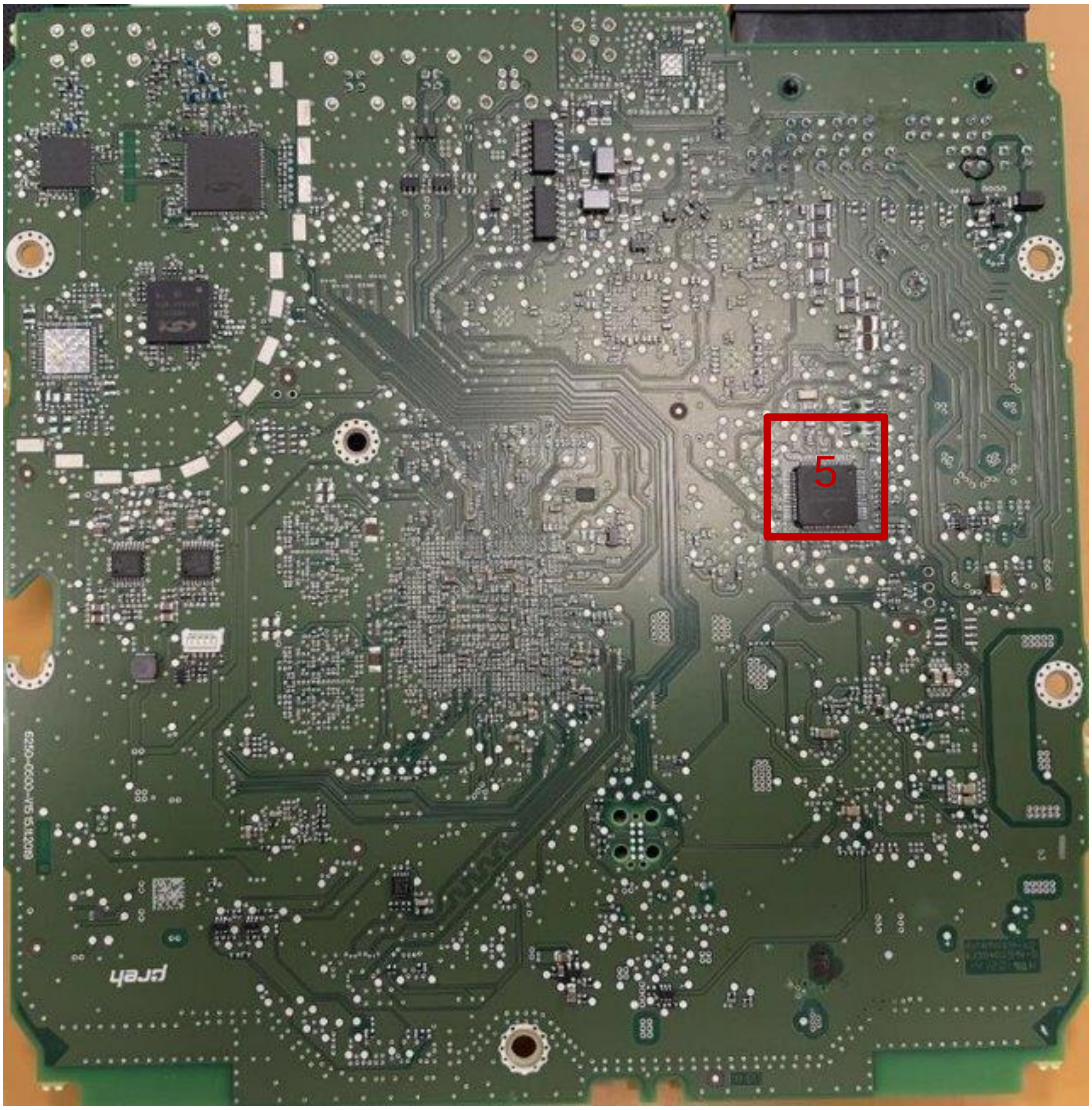
MySKODA application (source: Google Play Market)

The analyzed MIB3 infotainment unit manufactured by Preh GmBH (www.preh.com) had the following identifiers:

- Part number 3V0035820J
- Hardware version: H22
- Firmware version: 0304



MIB3 infotainment unit PCB. Side A



MIB3 infotainment unit PCB. Side B

Hardware components highlighted are:

1. R-Car M3 Main CPU (ARM64) Executes the main OS. Has a dedicated core CARCOM running real-time OS, which handles CAN bus communications.
2. eMMC with Linux FS.
3. SPI memory chip with low-level firmware.
4. WLAN and Bluetooth chip.
5. Power controller chip (PWC), ARM32.

SUMMARY

PCAutomotive identified multiple vulnerabilities with low-to-medium criticality, allowing a would-be attacker to get access to certain debug mechanisms of the MIB3 infotainment unit and cause its denial-of-service via in-vehicle Wi-Fi network. Certain issues were also identified in the OBD interface of Skoda and Volkswagen cars. Those allow a would-be attacker to successfully pass UDS authentication on the infotainment unit. All the issues related to the MIB3 unit affect Skoda and VW cars having this unit installed (3V0035820J H22 0304). Other MIB3 unit modifications were not tested against the identified issues.

Another issue in the OBD interface security control set allowed to issue a UDS command which caused vehicle engine and some other components to turn off while the vehicle is moving. Since one-time access to the in-vehicle OBD port is mandatory for successful exploitation, and since there exists additional exploitation restriction, the risk level was rated as medium. This vulnerability was tested on Skoda Superb III 2022. PCAutomotive assumes that some other Skoda and VW car models are also affected. PCAutomotive does not have the extensive list of affected car models.

Finally, two security issues were identified in Skoda cloud backend, which allowed a would-be attacker to obtain user nicknames and some vehicle data (mileage, recent trip duration, average and max. speed of the trip) by knowing only VIN number of a vehicle.

CVE ID	Title	CVSS 3.1 score
CVE not assigned	SWD debug interface available on infotainment ECU	Not calculated
CVE not assigned	Debug console on Power Controller Chip	Not calculated
CVE-2023-28895	Hard-coded password for access to power controller chip memory	3.5 (Low)
CVE-2023-28896	Weak encoding for password in UDS services	3.3 (Low)
CVE-2023-28897	Hard-coded password for UDS services	4.0 (Medium)
CVE-2023-28898	Head Unit Denial-of-Service via Apple CarPlay service	5.3 (Medium)
CVE-2023-28899	Denial of Service via ECU reset service	4.7 (Medium)
CVE-2023-28900	Nickname disclosure on the backend automotive server	5.3 (Medium)
CVE-2023-28901	Trip data disclosure on host fal-3a.prd.eu.dp.vwg-connect.com	5.3 (Medium)

DISCLOSURE TIMELINE

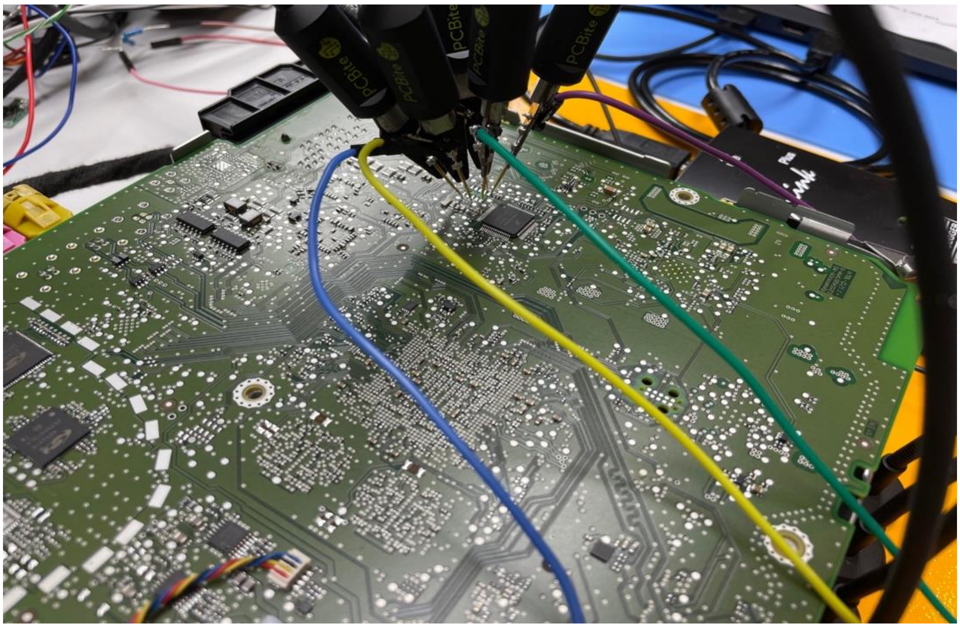
Date	Description
2022.11.21	Advisory sent to security@skoda-auto.cz
2022.12	Skoda fixed backend-related issues CVE-2023-28900 and CVE-2023-28901
2023.03.27	CVE numbers reserved by ASRG CNA
2023.07	Communication with Volkswagen before publishing the vulnerabilities
2023.09.14	Disclosure of the vulnerabilities at Secure Our Streets 2023

TECHNICAL DETAILS

SWD debug interface available on infotainment ECU

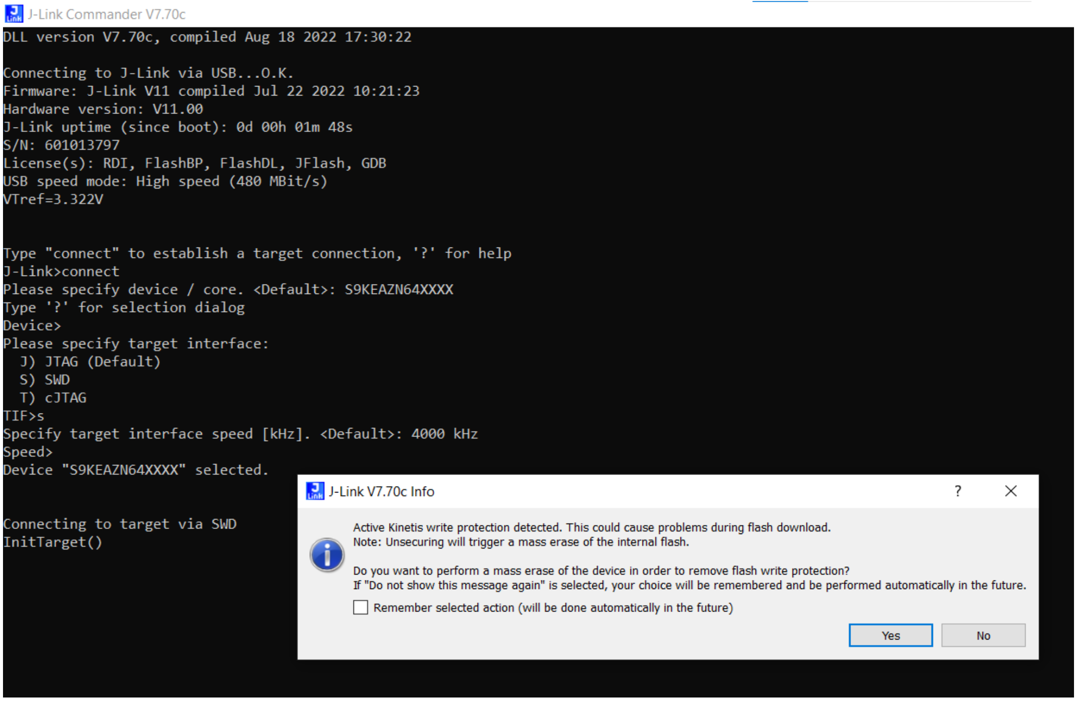
Description

IVI PCB contains power controller chip (PWC) S9KEAZN64A manufactured by NXP. This chip exposes working SWD debug interface on its pins. Debugging interface is protected though: prior to debugging the chip, it is required to perform erasing of firmware and configuration stored in internal memory of the chip. Nevertheless, it is possible to reprogram PWC with firmware from firmware update package after erase operation and get debug access to PWC.



Connection of a J-Link debugger to PWC

JTAG adapter, such as J-Link, can be used to connect to the SWD interface:



```
DLL version V7.70c, compiled Aug 18 2022 17:30:22

Connecting to J-Link via USB...O.K.
Firmware: J-Link V11 compiled Jul 22 2022 10:21:23
Hardware version: V11.00
J-Link uptime (since boot): 0d 00h 01m 48s
S/N: 601013797
License(s): RDI, FlashBP, FlashDL, JFlash, GDB
USB speed mode: High speed (480 MBit/s)
VTref=3.322V


Type "connect" to establish a target connection, '?' for help
J-Link>connect
Please specify device / core. <Default>: S9KEAZN64XXXX
Type '?' for selection dialog
Device>
Please specify target interface:
  J) JTAG (Default)
  S) SWD
  T) cJTAG
TIF>s
Specify target interface speed [kHz]. <Default>: 4000 kHz
Speed>
Device "S9KEAZN64XXXX" selected.


Connecting to target via SWD
InitTarget()
```

Active Kinetis write protection detected. This could cause problems during flash download.
Note: Unsecuring will trigger a mass erase of the internal flash.

Do you want to perform a mass erase of the device in order to remove flash write protection?
If "Do not show this message again" is selected, your choice will be remembered and be performed automatically in the future.

□ Remember selected action (will be done automatically in the future)

Connection of PWC SWD interface with J-Link adapter

The interface does not allow debugging due to enabled write-protection control. However, it does allow debugging after erasing the memory content of the PWC chip. The memory content can later be restored by writing back PWC firmware obtained from public sources, or by utilizing the vulnerability CVE-2023-28895.

Exploitation scenario and impact

Would-be attackers with physical access to the infotainment unit can unlock the SWD debug interface of the PWC chip. This potentially allows a slight attack surface increase.

CVE-2023-28895: Hard-coded password for access to PWC memory

Description

The PWC chip of the infotainment unit exposes an UART interface to the external socket of the unit, which supports the following debug commands:

```
* '?'/'h': help screen
* 'a': adc
* 'c*': pwc config
* 'C': pwc counters
* 'e'/'ec': uart statistics
* 'fx...': fake message from cc
* 'Fc': get flash crc
* 'ii'/'iw'/'ir': twi stuff
* 'm...': fake message to CARCOM
* 'M...': send debug input to CARCOM
* 'P1'/'P0': switch main power ON/OFF
* 'p': port states
* 'PWC:': switch (back) to pwc rx mode
* 'Q': switch to uart tunnel mode
* 'R1'/'R0': switch cpu reset
* 'u': updater stuff
* 'v': version infos
* 't...': time stuff
* 'T': print temperatures
* 'X...': force soft / sw / wd reset
```

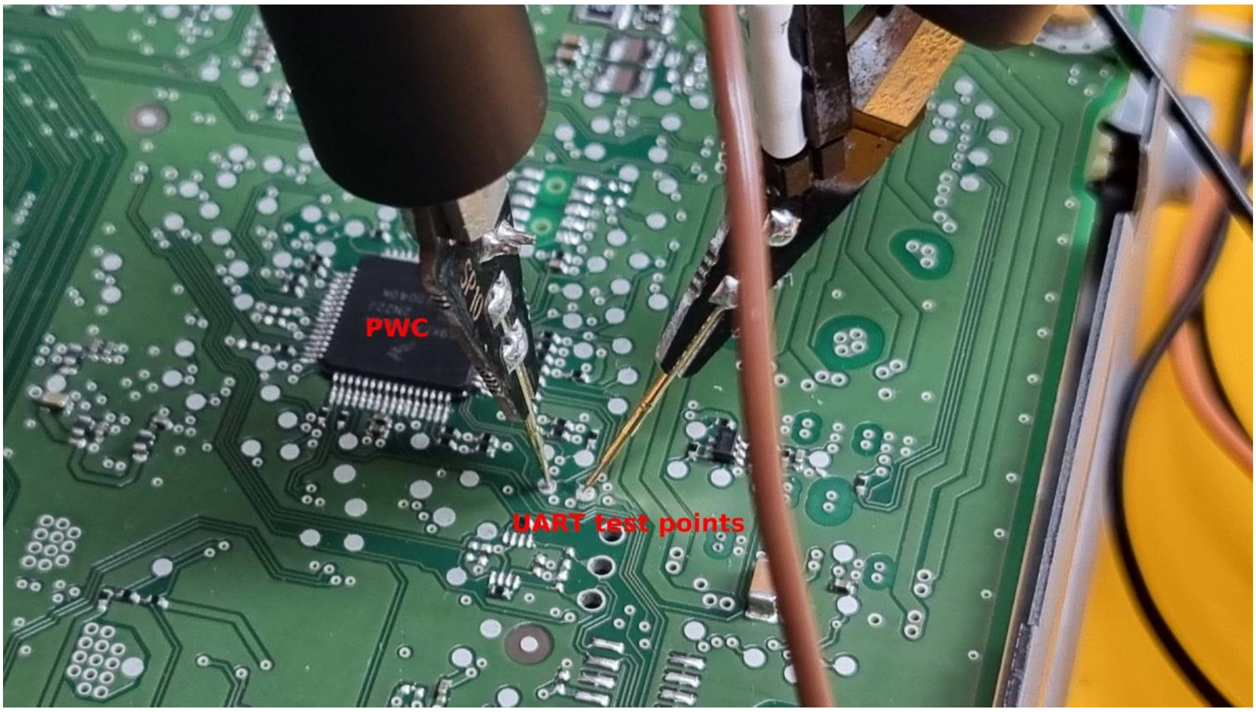
The console becomes available after sending a certain command to the PWC chip via another UART line connecting the PWC chip and the CARCOM core of the main CPU.

Exploitation scenario and impact

A would-be attacker with physical access to the infotainment unit can unlock the debug UART console of the PWC chip by issuing the following command to another UART line between the CARCOM core and the PWC chip:

```
0xF1 0x1D 0x01 0x01 <CHECKSUM 2 bytes> 0xF2.
```

Test pins of the UART line between PWC and CARCOM can be found on the infotainment system PCB:



Connection of the external UART interface to the UART1 line between PWC and CARCOM

From debug console, it is possible to access PWC firmware update functionality (console command ‘**u**') This command allows to read and modify PWC memory, thus extracting its firmware and writing an arbitrary binary code into the memory. The access is protected with the password which is hard-coded into PWC firmware (CVE-2023-28895). This potentially allows a slight attack surface increase.

CVE-2023-28896: Weak encoding for password in UDS services

CVE-2023-28897: Hard-coded password for UDS services

Description

UDS authentication for the infotainment unit is based on the following sequence of steps:

1. Request a random value (seed) from the infotainment unit.
2. Send an arithmetic addition of the static password value and the random value.

It is possible to retrieve the valid password from CAN bus traffic if it contains successful authentication attempts, by using a simple arithmetic subtraction (CVE-2023-28896). In addition to that, the password value is hard-coded into the firmware of the infotainment unit (CVE-2023-28897).

Exploitation scenario and impact

A would-be attacker with physical access to the OBD port can easily pass the UDS authentication on the infotainment unit and issue diagnostic commands to it. This potentially allows a slight attack surface increase.

CVE-2023-28898: Head Unit Denial-of-Service via Apple CarPlay service

Description

HTTP/RTSP service on port 7000/tcp which is available when the client is connected to vehicle's HU via CarPlay, incorrectly handles requests to the /logs scenario where id parameter is specified.

An attacker, who is connected to the same wireless network can send specially crafted request, for example, the following:

```
ANY /logs?id=0 RTSP/1.0
Host: 10.173.189.1:7000
```

In some cases, two consequent requests are required.

Exploitation scenario and impact

A would-be attacker with access to the in-vehicle Wi-Fi network can cause denial-of-service of the infotainment unit if Apple CarPlay interface between the infotainment unit and another device is established.

CVE-2023-28899: Denial of Service via ECU reset service

Description

Sending a certain broadcast UDS message to the OBD port of the vehicle causes some components in the vehicle to reset. As a result, the running engine immediately turns off, and most of the vehicle systems go offline and stop functioning for several seconds. Steering wheel and brakes remain operational. The impact can be achieved within certain short milage since the last activation of an undisclosed physical factor. However, under these conditions, the speed of the vehicle at which the attack works is not limited.

Exploitation scenario and impact

For exploitation, access to vehicle's OBDII port is required. Attackers who once gained short-term access to OBDII port, can install wireless (cellular, Wi-Fi, or Bluetooth) interface device, gaining persistent access to vehicle diagnostic interface, and an ability to shut down vehicle engine at any speed within a short mileage.

CVE-2023-28900: Nickname disclosure on Skoda Connect backend automotive server

CVE-2023-28901: Trip data disclosure on Skoda Connect backend automotive server

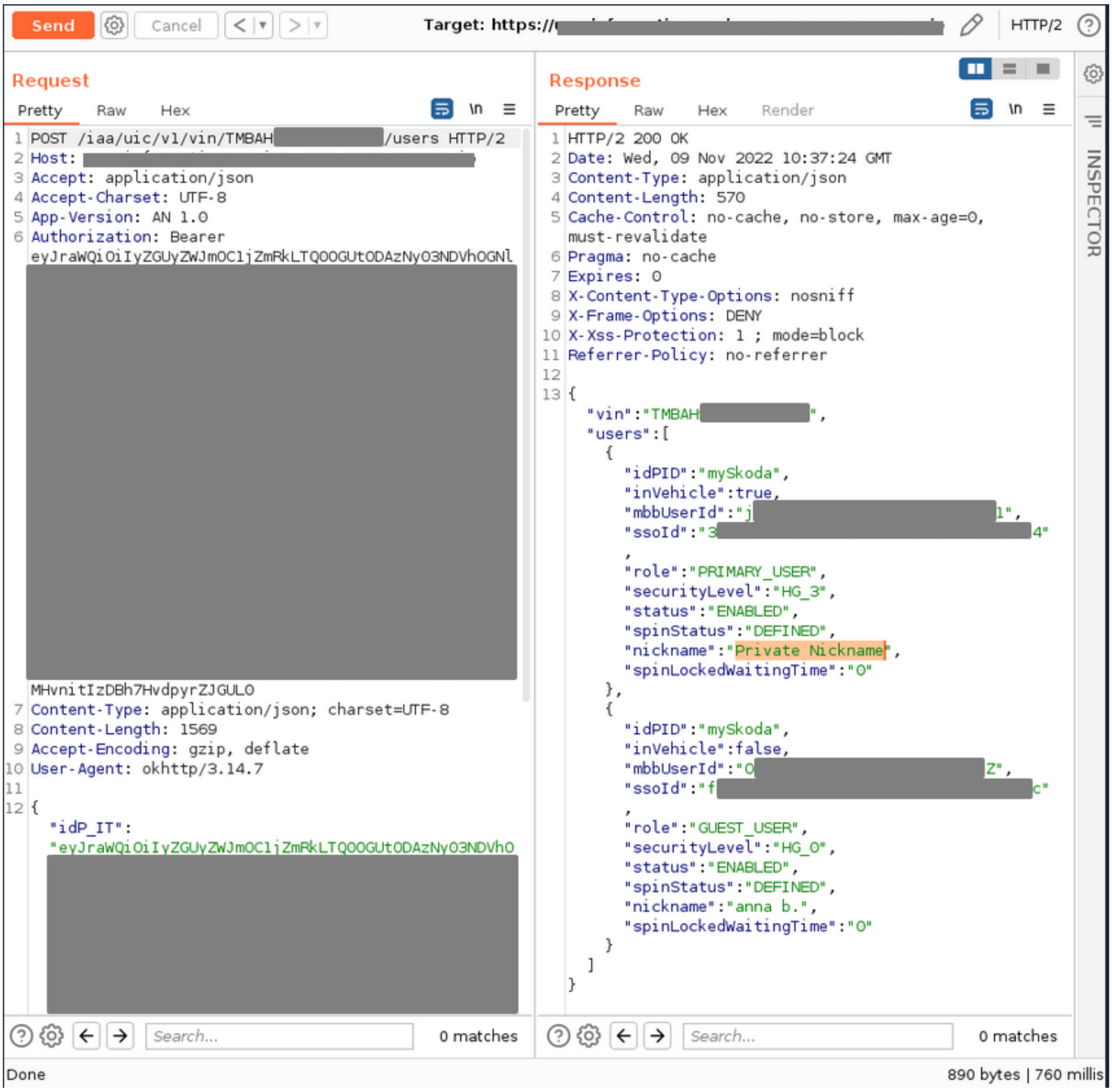
Description

An attacker can receive nickname and other identifiers of Skoda Connect users by arbitrary VIN number (CVE-2023-28900). This issue is categorized as Broken Access Control vulnerability. An attacker can act outside of the intended permissions that allows him to get extended information on the car's owner.

An attacker can receive trip details by Skoda vehicle VIN number, if the primary user is registered in the vehicle (CVE-2023-28901). This issue is categorized as Broken Access Control vulnerability. An attacker can act outside of the intended permissions that allows him to get information on trip timestamps, fuel consumption, speed, etc.

Exploitation scenario and impact

A remote attacker can reveal Skoda vehicle user's data, including usernames, and information about their recent trips, by issuing certain requests to Skoda backend API endpoints.



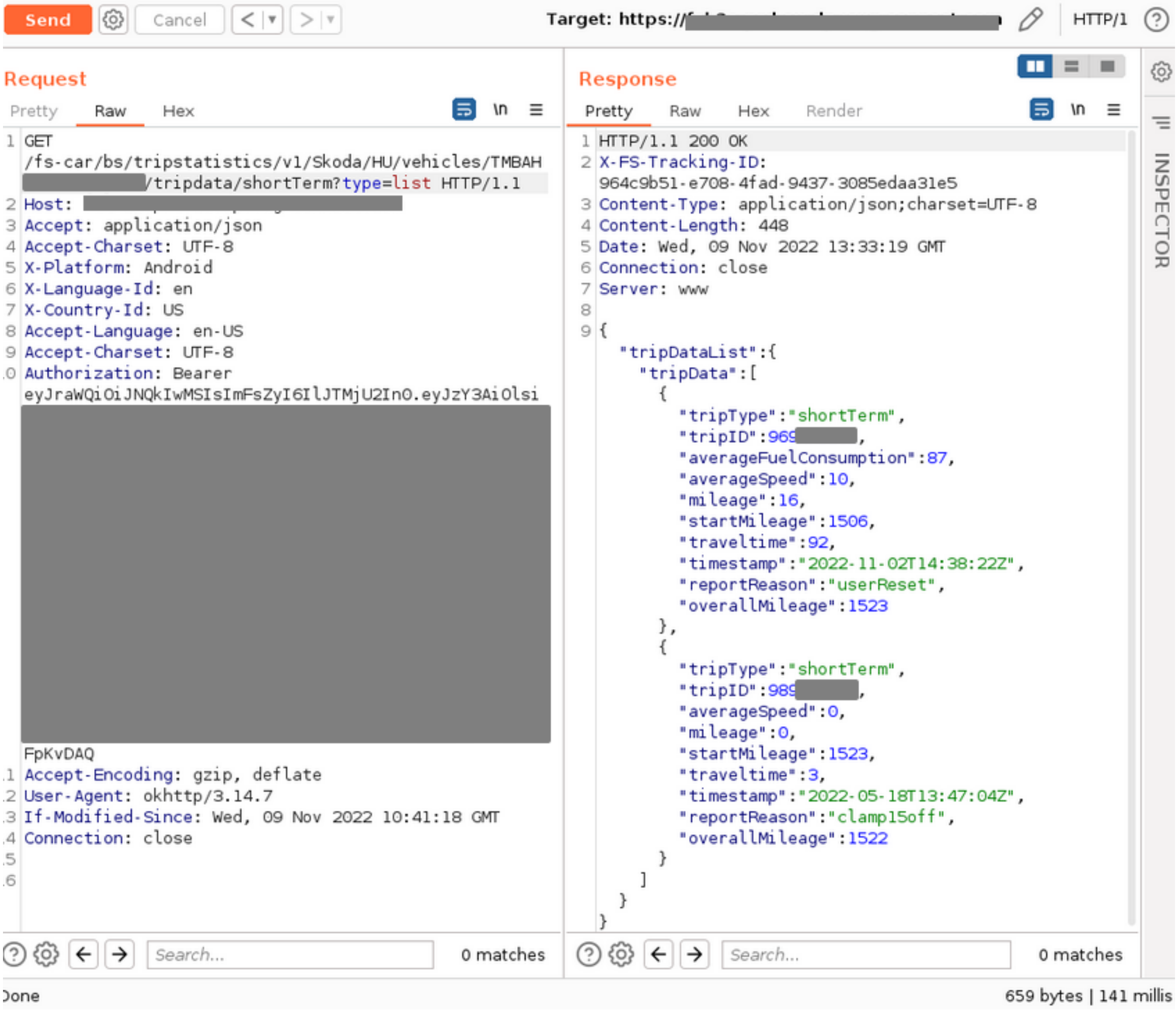
```
POST /iaa/uic/v1/vin/TMBAH[redacted]/users HTTP/2
Host: [redacted]
Accept: application/json
Accept-Charset: UTF-8
App-Version: AN 1.0
Authorization: Bearer
eyJraWQiOiIyZGUyZWJmOC1jZmRkLTQ0OGUtODAzNy03NDVhOGNl
[redacted]
MHvnitIzDBh7HvdpyrZJGUL0
Content-Type: application/json; charset=UTF-8
Content-Length: 1569
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.14.7

{
  "idP_IT":
  "eyJraWQiOiIyZGUyZWJmOC1jZmRkLTQ0OGUtODAzNy03NDVhO
  [redacted]
```

```
HTTP/2 200 OK
Date: Wed, 09 Nov 2022 10:37:24 GMT
Content-Type: application/json
Content-Length: 570
Cache-Control: no-cache, no-store, max-age=0,
must-revalidate
Pragma: no-cache
Expires: 0
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1 ; mode=block
Referrer-Policy: no-referrer

{
  "vin":"TMBAH[redacted]",
  "users":[
    {
      "idPID":"mySkoda",
      "inVehicle":true,
      "mbbUserId":"j[redacted]l",
      "ssoId":"3[redacted]4"
      ,
      "role":"PRIMARY_USER",
      "securityLevel":"HG_3",
      "status":"ENABLED",
      "spinStatus":"DEFINED",
      "nickname":"Private Nickname",
      "spinLockedWaitingTime":"0"
    },
    {
      "idPID":"mySkoda",
      "inVehicle":false,
      "mbbUserId":"0[redacted]Z",
      "ssoId":"f[redacted]c"
      ,
      "role":"GUEST_USER",
      "securityLevel":"HG_0",
      "status":"ENABLED",
      "spinStatus":"DEFINED",
      "nickname":"anna b.",
      "spinLockedWaitingTime":"0"
    }
  ]
}
```

Retrieving usernames of users registered as owners of the vehicle by VIN number



```
GET
/fs-car/bs/tripstatistics/v1/Skoda/HU/vehicles/TMBAH
[redacted]/tripdata/shortTerm?type=list HTTP/1.1
Host: [redacted]
Accept: application/json
Accept-Charset: UTF-8
X-Platform: Android
X-Language-Id: en
X-Country-Id: US
Accept-Language: en-US
Accept-Charset: UTF-8
Authorization: Bearer
eyJraWQiOiJNQkIwMSIsImFsZyI6IlJTMjU2In0.eyJzY3AiOlsi
[redacted]
FpKvDAQ
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.14.7
If-Modified-Since: Wed, 09 Nov 2022 10:41:18 GMT
Connection: close
```

```
HTTP/1.1 200 OK
X-FS-Tracking-ID:
964c9b51-e708-4fad-9437-3085edaa31e5
Content-Type: application/json;charset=UTF-8
Content-Length: 448
Date: Wed, 09 Nov 2022 13:33:19 GMT
Connection: close
Server: www

{
  "tripDataList":{
    "tripData":[
      {
        "tripType":"shortTerm",
        "tripID":969[redacted],
        "averageFuelConsumption":87,
        "averageSpeed":10,
        "mileage":16,
        "startMileage":1506,
        "traveltime":92,
        "timestamp":"2022-11-02T14:38:22Z",
        "reportReason":"userReset",
        "overallMileage":1523
      },
      {
        "tripType":"shortTerm",
        "tripID":989[redacted],
        "averageSpeed":0,
        "mileage":0,
        "startMileage":1523,
        "traveltime":3,
        "timestamp":"2022-05-18T13:47:04Z",
        "reportReason":"clamp15off",
        "overallMileage":1522
      }
    ]
  }
}
```

Retrieving trip data of the Skoda vehicle by VIN number

SECURITY FIXES AND RECOMMENDATIONS

The backend-related issues (CVE-2023-28900, CVE-2023-28901) are fixed.

PCAutomotive does not possess any information regarding fixing other identified issues.

CREDITS

Abdellah Benotsmane
Aleksei Stennikov
Anna Breeva
Artem Ivachev

Danila Parnishchev

Mikhail Evdokimov

Polina Smirnova