SIB 65 15 19 2019-08-07

SECURITY IMPROVEMENTS FOR CONNECTEDDRIVE

MODEL

Engineering Designation	Model Description	Model Year
F01, F02	7 Series Sedan including ALPINA B7	2011 to 2015
F04	7 Series ActiveHybrid	2011 to 2012
F06	6 Series Gran Coupe including ALPINA B6	2013 to 2019
F07	5 Series Gran Turismo	2011 to 2017
F10	5 Series Sedan	2011 to 2016
F12	6 Series Convertible	2012 to 2018
F13	6 Series Coupe	2012 to 2017
F15	X5 Sport Activity Vehicle	2014 to 2018
F16	X6 Sport Activity Coupe	2015 to 2019
F22	2 Series Coupe	2014 to 2019
F23	2 Series Convertible	2015 to 2019
F25	X3 Sport Activity Vehicle	2011 to 2017
F26	X4 Sport Activity Coupe	2015 to 2019
F30	3 Series Sedan	2012 to 2018
F31	3 Series Sports Wagon	2014 to 2019
F32	4 Series Coupe	2014 to 2019
F33	4 Series Convertible	2014 to 2019
F34	3 Series Gran Turismo	2014 to 2019
F36	4 Series Gran Coupe	2015 to 2019
F39	X2 SAV	2018 and 2019
F48	X1 SAV	2016 to 2019
F80	M3 Sedan	2015 to 2018
F82	M4 Coupe	2015 to 2019
F83	M4 Convertible	2015 to 2019
F85	X5 M SAV	2015 to 2018
F86	X6 M SAC	2015 to 2019
F87	M2 Coupe	2016 to 2019
F90	M5 Sedan	2018 and 2019
G01	X3 SAV	2018 and 2019
G02	X4 SAC	2019
G12	7 Series Sedan including ALPINA B7	2016 to 2019
G30	5 Series Sedan	2017 to 2019
G32	6 Series Gran Turismo	2018 and 2019
I01	i3	2014 to 2019
I12	i8 Coupe	2014 to 2019
I15	i8 Roadster	2019

SITUATION

Security vulnerabilities in BMW infotainment control units have been identified in vehicles equipped with ID4 (Entry Nav or Entry Media or NBT) and ID5/ID6 (NBT EVO) head units.

Note: ID7 MGU (HU-H3 iDrive7 Media Graphics Unit) and Entry EVO Nav or Entry EVO Media are not affected.

CAUSE

A Chinese cybersecurity research team Tencent Keen Security Lab (“Tencent”) examined various BMW models for potential security vulnerabilities from January 2017 to February 2018. They identified and informed the BMW Group of 14 vulnerabilities, five of them remotely via a mobile communications base station that was set up specifically for the research work.

The relevant configuration changes to the security parameters were transferred via the BMW Group IT back end to the affected vehicles by means of "over the air" vehicle provisioning. In addition to the measures already implemented via the ConnectedDrive back end, a software update is also available depending on the head-unit generation.

The update measures mentioned below are available for vehicles with an active ConnectedDrive/telematics services contract that are equipped with one of the following types of optional equipment:

- SA6AE Teleservices

or

- SA6NL Connect. Bluetooth and USB devices incl.

CORRECTION

- Check and update head unit software
- Install KISU update (Customer Initiated Software Update) depending on head unit installed as outlined in the procedure below

PROCEDURE

Review and perform this procedure only on vehicles equipped with ID4 (Entry Nav or Entry Media or NBT) and ID5/ID6 (NBT EVO) head units.

1. Check the I-level of the vehicle (AIR, Key read or Remote Key Read). Make note of the I-level.

2. Perform a vehicle test with ISTA. Once the vehicle test is performed, hover your mouse pointer over the head unit as shown below. This provides the following details:

   a. The head unit variant installed in the vehicle (arrow)

   b. The HWEL (hardware electronics) number. If the vehicle is equipped with an RSE (Rear Seat Entertainment), also check the last numbers starting with “RSE…” in the respective column below.

3. Is the HWEL version readout from the vehicle listed below for the corresponding head unit?

ID4 Entry Nav / Entry Media	ID4 HU-H & HU-H Rear Seat Entertainment (RSE)	ID4 HU-H (EVO)	ID5 / ID6 NBTEVO & Rear Seat Entertainment (RSE)
HWEL-0000116C	HWEL-00000DF5	HWEL-000022E3	HWEL-00002479
HWEL-0000116E	HWEL-00000DF6	HWEL-000022E4	HWEL-0000247A
HWEL-00001703	HWEL-00000DF7	HWEL-000022E5	HWEL-0000247B
HWEL-00001704	HWEL-00000DF8	HWEL-000022E6	HWEL-000026B9
HWEL-00001705	HWEL-00000DFF	HWEL-000022E7	HWEL-000026BA
HWEL-00001706	HWEL-00001018	HWEL-000022E8	HWEL-000026BB
HWEL-000019F9	HWEL-00001019	HWEL-000031DC	HWEL-00002AB8
HWEL-000019FA	HWEL-0000101A	HWEL-000031DD	HWEL-00002AB9
HWEL-000019FC	HWEL-00001294	HWEL-000031DE	HWEL-00002C14
HWEL-0000274C	HWEL-00001295	HWEL-000031DF	HWEL-00002FC2
HWEL-0000274D	HWEL-00001296	HWEL-000031E0	HWEL-00002FC3
HWEL-0000274E	HWEL-000018C2	HWEL-000031E1	HWEL-00002FC4
HWEL-0000274F	HWEL-000018C3		HWEL-00002FC5

HWEL-00002750 HWEL-00002753 HWEL-00002754 HWEL-00001170 HWEL-00001707 HWEL-00001708 HWEL-00001709 HWEL-000019F7 HWEL-000019F8 HWEL-000019FB HWEL-00002746 HWEL-00002747 HWEL-00002748 HWEL-00002749 HWEL-0000274A HWEL-0000274B HWEL-00002751 HWEL-00002752 HWEL-00002755	HWEL-00001A41 HWEL-00001A42 HWEL-00001A43 HWEL-00001A44 HWEL-00001A45 RSE HWEL-00000E66 RSE HWEL-00000F5E RSE HWEL-00000F5F		HWEL-00003A09 HWEL-00003A0A HWEL-00003A0B HWEL-00003A0C HWEL-00003A0D HWEL-00003A0E RSE HWEL-00001EF7 RSE HWEL-00001EFB

a. Yes: Proceed to the steps below relating to the specific head unit installed in the vehicle being serviced.

b. No: No further action is needed because the control module installed in the vehicle is not affected.

Steps for ID4 (Entry Nav, Entry Media, HU-H & HU-H EVO) head units

4. Was the vehicle last treated with ISTA 4.16.1 or higher, and is the I-level 19-03-5xx or higher??

5. YES: The vehicle already has the software that provides the vehicle with added security measures installed. Continue with step 7 below.

6. NO: Program and encode the vehicle using ISTA 4.16.1 or higher (released early March, 2019).

7. Download and install the “Customer initiated update software” (KISU software) in the vehicle.

   a. Refer to the instructions below “updating KISU data”

Steps for ID5 / ID6 NBT EVO (HU-H2) head unit:

8. Was the vehicle last treated with ISTA 4.01.1 or higher and is the I-level 16-07-500 or higher??

9. YES: The vehicle already has the software that provides the vehicle with added security measures. No further actions required.

10. NO: Program the vehicle with ISTA 4.01.1 or higher.

Note that ISTA will automatically reprogram and code all programmable control modules that do not have the latest software.

Always connect a BMW approved battery charger/power supply (SI B04 23 10).

For information on programming and coding with ISTA, refer to CenterNet / TIS / Technical Documentation / Vehicle Programming.

Steps for installing the Customer-initiated software update (KISU)

Downloading Customer-initiated software update on to a USB.

1. Prerequisites:

   - USB stick with at least 500 MB of free memory and formatted as FAT16, FAT32 or NTFS filesystem.

   - Access to a computer with internet access.
   - The 17-digit vehicle identification number (VIN) of the customer vehicle.

2. Download software:

   - Open the website: https://www.bmw.com/update
   - Enter the 17-digit vehicle identification number (VIN).
   - If the update is available, download the software (example: UPD 09042.bin) onto the USB stick.

3. Installation in the vehicle – updating of head unit:

   - Vehicle must have the minimum I-level specified in this bulletin.
   - Connect the USB in the center console of the vehicle.
   - Then install the software in the vehicle ("iDrive settings" / "Software update").

WARRANTY INFORMATION

Covered, one-time, under the terms of the BMW New Vehicle Limited Warranty for Passenger Cars and Light Trucks.

Defect Code:	**8411900100**	

The vehicle is already in the workshop, or if applicable, completion before the first delivery of the vehicle

Work Pkg	Labor Operation:	Labor Allowance:	Description (Plus work):
# 1	00 66 667	Refer to AIR	Programming and encoding the vehicle only (includes connecting an approved battery charger/power supply and performing a vehicle test)
Or:			
# 2	00 66 668	Refer to AIR	Programming and encoding the vehicle (includes connecting an approved battery charger/power supply and performing a vehicle test) and installing customer-initiated software update (KISU data)
Or:			
# 3	00 66 669	Refer to AIR	Installing customer-initiated software update (KISU data) (The vehicle is already at the specified Target integration level or higher)

If you are using a Main labor code for another repair, use the Plus code labor operation above that applies instead of the Main labor code.

Or:

The vehicle arrives at your center, this action applies and it has not been previously performed (No other Main work will be performed/claimed during this workshop visit)

Work Pkg	Labor Operation:	Labor Allowance:	Description (Main work):
# 4	00 66 090	Refer to AIR	Programming and encoding the vehicle only (includes connecting an approved battery charger/power supply and performing a vehicle test)
Or:			
# 5	00 66 091	Refer to AIR	Programming and encoding the vehicle (includes connecting an approved battery charger/power supply and performing a vehicle test) and installing customer-initiated software update (KISU data)
Or:			
# 6	00 66 092	Refer to AIR	Installing customer-initiated software update (KISU data) (The vehicle is already at the specified Target integration level or higher)

Refer to AIR for the corresponding flat rate unit (FRU) allowances.

During the same workshop visit, **if a vehicle also requires another Technical Campaign or repair that also includes programming and encoding the control units, the programming procedure may only be invoiced one time.**

Claim Repair Comments

Unless additional related/in conjunction work was required (not addressed and/or included in one of the options provided above), then only reference the SIB number and the work package (Pkg) number performed in the RO technician notes and in the claim comments (For example: B65 15 19 WP 1).

Programming and Encoding - Vehicle Control Units (RO and Claim Comments Required)

The programming procedure automatically reprograms and encodes all vehicle control modules which do not have the latest software i-level. If one or more control module failures occur during this programming procedure:

> Please claim this consequential control module-related repair work under the defect code listed in this bulletin with the applicable AIR labor operations.

Please explain this additional work (The why and what) on the repair order and in the claim comments section.

For control module failures that occurred prior to performing this programming procedure:

> When covered under an applicable limited warranty, claim this control module-related repair work using the applicable defect code and labor operations (including diagnosis) in AIR.

Supporting Materials

picture_as_pdf B651519_Q_A attachment.pdf

Q&A – Security Vulnerabilities in Vehicles equipped with ConnectedDrive

1. What vulnerabilities were identified?
Potential vulnerabilities were identified in BMW Vehicles by Tencent's Keen Security Lab ("Tencent') during extensive testing and research of the BMW ConnectedDrive system and related infotainment components in the vehicle.

2. What Was the Risk?
No drivers or road users were ever at risk. Tencent research showed, that a successful exploitation of the vulnerabilities required among other things, mastering a long, complex exploit chain, access to specific vehicle components, action by the attacker as well as the driver, in order to pose a risk. Some of the vulnerabilities also required a physical connection, which required an adversary to gain access to the vehicle's interior.

3. How were the vulnerabilities addressed?
Countermeasures were developed and rolled out via BMW Group systems to vehicles by over-the air updates. Additional software updates are available at BMW centers to close potential non-critical vulnerabilities and increase the vehicle's overall robustness.

4. Are the vehicles still at risk?
Remote vulnerabilities were remediated with the highest priority. BMW has also issued optional security updates which are available at BMW centers. Please contact your local BMW center for further information.

5. As a customer, how can I find out if my car is affected or if it needs an update?
Only vehicles equipped with ConnectedDrive were affected. Fixes for remote vulnerabilities were already rolled out via the BMW Group backend servers systems to vehicles by over-the-air mobile connection. Vehicles built in model year 2019 and later have the latest updates installed.

In addition, security patches in the form of software updates are available for non-critical vulnerabilities. These updates are available for the applicable BMW models at BMW centers and can be installed at your next regular service visit.

7. What risks remain after all the countermeasures have been implemented?
The vulnerabilities no longer pose a risk.