BMW Connected Drive security loopholes

ADAC finds: more than 2.2m vehicles affected world-wide

1. Background

The BMW Connected Drive system enables vehicles to exchange data wirelessly (by means of a permanently installed SIM card) with the car manufacturer (such as – depending on the model and country – inspection due dates, battery status, traffic jam data, roadside assistance calls, etc.). Moreover, there is a smartphone app for sending commands, such as “open driver’s door”, “activate horn”, etc., to the vehicle via a manufacturer-operated server.
This technology gives the manufacturer several years’ head start over the competition. Moreover, it anticipates functions that will be launched on a larger scale with the introduction of eCall by April 2018. One such function is bCall (roadside assistance and workshop call), which will have an impact on independent workshops’ non-discriminatory access to the market.
For the above reasons, ADAC commissioned an external expert to analyse the information which vehicles transmit to the manufacturer via BMW Connected Drive when an inspection or repair is due. The objective was to determine whether independent workshops might be at a disadvantage and whether ADAC should step in to protect consumer interests.
Although this was never intended, the investigations revealed security loopholes, prompting the publication of the findings below.

2. Key story

ADAC has found security loopholes in BMW Connected Drive-equipped vehicles. It only takes one-time preparation and a few minutes to open cars by mobile phone without leaving any traces. According to BMW, this problem affects 2.2 million vehicles of numerous model series manufactured under the BMW, Mini and Rolls Royce brands (see enclosed list).

In its capacity as a consumer protection organisation, ADAC has requested BMW to close these security loopholes immediately and report on the developments. BMW has announced that the security loopholes will be closed by 31 January 2015 by activating encrypted communication with the vehicle.

To discourage copycats and avoid exposing the vehicles of the consumers concerned to an increased break-in and theft risk, ADAC has delayed publication of its findings until the security loophole is closed by the manufacturer. ADAC is currently not aware of any criminal offenses perpetrated using these loopholes.

Vehicle owners cannot identify whether their vehicle has already been processed because this is done unnoticed by wireless communication. If you want to be certain, call the BMW hotline at **xxx/yyyyyyyy *(differs from country to country)*** – or go to a BMW dealer. We especially recommend this for vehicles which, in recent months, have been parked in underground car parks or in other locations with no mobile phone reception or whose starter battery was temporarily disconnected. BMW are unable connect to these cars.

This is the first-ever “digital recall” requiring neither a workshop call nor replacement of any parts.

ADAC Technical Zentrum, Arnulf Volkmar Thiemel, +49 8191 93 86 96
Otto-Lilienthal-Strasse 2, 86899 Landsberg a. Lech

arnulf.thiemel@tzll.adac.de

ADAC demands state-of-the-art protection of in-car computer technology against manipulation and illegal access. Such protection must be based on standards long since operative in other industries (e.g. IT industry). Moreover, said protection needs to be confirmed by an impartial body, e.g. via Common Criteria certification through the Federal Office for Information Security (BSI) in Bonn, Germany – or related organisations in other countries (refer to www.commoncriterialportal.org).

3. Affected vehicles (according to manufacturer)

All Connected Drive models produced from March 2010 up to, and including, 8 December 2014.

BMW
1-series, incl. Cabrio, Coupé and Touring (E81, E82, E87, E88, F20, F21)
2-series, incl. Active Tourer, Coupé and Cabrio (F22, F23, F45)
3-series, incl. Cabrio, Coupé, GT, M3 and Touring (E90, E91, E92, E93, F30, F31, F34, F80)
4-series Coupé, Cabrio, GranCoupé and M4 (F32, F33, F36, F82, F83)
5-series, incl. GT and Touring (E81, E82, F07, F10, F11, F18)
6-series, incl. Cabrio and GranCoupé (F06, F12, F13)
7-series (F01, F02, F03, F04)
I3 (I01), I8 (I12)
X1 (E84), X3 (F25), X4 (F26), X 5 (E70, F15, F85), X6 (E71, E72, F16, F86), Z4 (E89)

Mini
3-door and Countryman (F56, F60)

Rolls Royce
Phantom, incl. Coupé and Drophead Coupé (RR1, RR2, RR3)
Ghost (RR4)
Wraith (RR5)

The loopholes apply to 423,000 vehicles in Germany, 1.2m in Europe an 2.2m world-wide. The manufacturer claims that any vehicles produced on or after 9 December 2014 do not have these loopholes.

BMW will wirelessly switch the affected vehicles to encrypted communication and expects to complete most of the switch by 31 January 2015. No workshop call will be required, and no parts or software will have to be exchanged.

BMW claims to have informed the German Federal Motor Transport Authority (KBA).

4. Background information: Specific security loopholes found by ADAC

Remote Services: unauthorised execution of remote functions, e.g. opening doors

Last State Call: Spotting the position of the vehicle and whether it is locked or unlocked

Real Time Traffic Information (RTTI): Monitoring current vehicle positions and, e.g., recorded speed data; tracking vehicles (data protection!)

Intelligent Emergency Call: phone numbers stored in the ECU, e.g. emergency numbers, can be changed

BMW Online: Eavesdropping on private e-mails (data protection!)

5. Recommendations for FIA partner clubs

We recommend to contact your national importers and ask how they are handling the matter. Insist that a telephone hotline should be established in each country, allowing the owners of any affected vehicles to find out whether their vehicles have already been processed, i.e. whether the manufacturer has already wirelessly activated encryption.

ADAC Technical Zentrum, Arnulf Volkmar Thiemel, +49 8191 93 86 96
Otto-Lilienthal-Strasse 2, 86899 Landsberg a. Lech

arnulf.thiemel@tzll.adac.de