Technical product information

Topic	Suspicion that control units or services have been influenced by third parties
Market area	Russische Föderation (5RU),Australia E04 Bentley rest Asia and Australia (6E04),China 796 VW Import Comp. Ltd (Vico), Beijing (6796),Germany E02 Bentley rest Europe (6E02),Japan E03 Bentley Japan (6E03),Korea, (South) E08 Bentley South Korea (6E08),United Arab Emirates E06 Bentley Middle East and Africa (6E06),United Kingdom E01 Bentley UK (6E01),United States E05 Bentley USA and rest America (6E05)
Brand	Bentley
Transaction No.	2065604/1
Level	EH
Status	Approval
Release date	

New customer code

Object of complaint	Complaint type	Position
information, navigation, communication, entertainment -> mobile telephone functions, customer portal, applications -> application for mobile device (app)	control units, services -> Influence by third parties	
information, navigation, communication, entertainment -> mobile telephone functions, customer portal, applications -> customer portal application	control units, services -> Influence by third parties	
body fixtures and fittings -> window opening/closing, window heating -> electric window lifter	control units, services -> Influence by third parties	
access control, driving authorisation, antitheft protection -> vehicle locking/unlocking -> door unlocking	control units, services -> Influence by third parties	
information, navigation, communication, entertainment -> instrument displays -> instrument panel display	control units, services -> Influence by third parties	
information, navigation, communication, entertainment -> traffic information system -> display traffic information (TMC)	control units, services -> Influence by third parties	
information, navigation, communication, entertainment -> traffic information system -> display traffic information (online)	control units, services -> Influence by third parties	
information, navigation, communication, entertainment -> radio, navigation, MMI, hard drive device functions -> monitor display	control units, services -> Influence by third parties	
information, navigation, communication, entertainment -> audio playback, audio settings -> audio playback	control units, services -> Influence by third parties	
information, navigation, communication, entertainment -> driver information system (DIS, MFI, MMI) -> information system display	control units, services -> Influence by third parties	
information, navigation, communication, entertainment -> online services -> privacy settings	control units, services -> Influence by third parties	
information, navigation, communication, entertainment -> windscreen projection (Head-up Display) -> windscreen projection display (Head-up Display)	control units, services -> Influence by third parties	
access control, driving authorisation, antitheft protection -> vehicle locking/unlocking -> door locking	control units, services -> Influence by third parties	
access control, driving authorisation, antitheft protection -> vehicle locking/unlocking -> rear lid unlocking	control units, services -> Influence by third parties	
access control, driving authorisation, antitheft protection -> vehicle locking/unlocking -> rear lid locking	control units, services -> Influence by third parties	

Vehicle data

Bentley

Sales types

Type	MY	Brand	Designation	Engine code	Gearbox code	Final drive code
*	2010	E		*	*	*
*	2011	E		*	*	*
*	2012	E		*	*	*
*	2013	E		*	*	*
*	2014	E		*	*	*
*	2015	E		*	*	*
*	2016	E		*	*	*
*	2017	E		*	*	*
*	2018	E		*	*	*
*	2019	E		*	*	*

*	2020	E		*	*	*
*	2021	E		*	*	*
*	2022	E		*	*	*
*	2023	E		*	*	*

Documents

Document name
master.xml
securityquestionnaire.pdf

Customer statement / workshop findings

In the event a customer complaint is received relating to a suspicion that control units or services have been influenced by third parties the instructions within this TPI should be followed

Important customer management information

- Remain calm and handle customer concerns in the same professional manner all other concerns are handled
- The customer may need to be calmed down. Please do not use any alarming language, such as “you have been hacked.”
- Take notes of all details that the customer tells you during the course of the conversation. Remain objective.
- Give the customer confidence that you can resolve their concerns.
- Assure the customer that all concerns will be handled in accordance with all current defined processes

▪

NOTE: The date and time that a complaint was observed are always required for further analysis. This also applies for permanent complaints

- Check to confirm if the customer complaint matches a VIN applicable TPI, if so, observe and fully perform the information/instructions provided
- Check to confirm if it is possible to rule out incorrect operation by the user
- Check to confirm if a technical or functional malfunction can be identified as the cause of the complaint
- Review the Product Cyber Security and Software Updates Frequently Asked Questions which can be seen in the Customer information section of this TPI

NOTE: If a technical cause for the complaint was identified in any of the previous points (for example the influence from third parties is no longer suspected), this TPI is not relevant for the complaint in question, you can now proceed with normal diagnosis

Technical background

A suspicion that control units or services have been influenced by third parties means that unauthorised people or groups may have gained access to a vehicle’s control unit(s) or online services and may have manipulated them in such a way that may compromise customer data confidentiality or the operation of the vehicle and/or online services.

When investigating potential third party influences of control units or online services, it is important to take all normal diagnostic measures to rule out a normal functional error or misuse of the system by the user

Some DTC’s may be stored depending on the nature of the incident, however it is possible that a control unit or service can be influenced in such a way that does not store any DTC’s

Bentley Motors work from the assumption that an attack will generally not be immediately detectable

As per the mandatory reporting list, it is mandatory to report suspicion that a control unit or service has been influenced in an unauthorised manner by a third party, once normal diagnosis has confirmed there is no user error or standard functional issue.

▪

Complete and return the attached questionnaire to help with complaints where a suspicion is evident regarding control units or services which may have been influenced by third parties

Production change

Not applicable

Measure

1) Complete the attached questionnaire

VERY IMPORTANT: Once the questionnaire is complete please save a copy and attach to a new or existing Technical DISS query as detailed below

Instances where there is a suspicion that control units or services have been influenced by third parties: It is only necessary to send a cyber security DISS query to Bentley in order to resolve the customer complaint if the possibility of technical malfunction has been excluded and there is a suspicion that control units or services have been influenced by third parties in an unauthorised manner. When creating a cyber security Technical DISS query, please observe the following instructions:

I nstructions for creating a cyber security DISS Technical Query

When coding the complaint on DISS from a customer perspective, use the “control units, services -> Influence by third parties suspected” complaint type (as detailed in the header of this TPI). This helps immediately raise to Bentley Product Support that you suspect a third party may have influenced a control unit or service and further investigation is required.

You must also attach to the DISS an up-to-date and full diagnostic log. The customer questionnaire, completed to the fullest extent possible, must also be attached along with any other relevant images, videos, documents and diagnosis/repair information to support investigation of the concern.

Customer information

Modern vehicles are becoming increasingly complex and digital. This is especially the case when it comes to features that network vehicles with other road users or traffic infrastructure outside the vehicle.

Hackers aim to find a weakness in the system and manipulate it in a way that may cause damage. However, this damage may look exactly the same as a malfunction with a "normal" technical cause, such as a partial hardware failure. For this reason, a suspected exploitation of a weakness is known as a cyber security event.

If a suspected exploitation of a weakness is confirmed, it then becomes known as a cyber security incident.

Bentley Motors can perform an initial analysis of the vehicle to find out whether the cause of the behaviour described lies in the function itself, whether there are other causes or whether a suspected cyber security incident should be investigated further.

FAQs about cybersecurity and software updates

Cybersecurity

1) What is a cybersecurity incident?

A cybersecurity incident is when a hacker exploits a vulnerability to impact data security or vehicle functions, for example.

One point to note is that you will not generally be able to detect an incident, as the effects may appear to you to be identical to a problem with a "normal" cause such as the partial failure of a hardware component.

2) What do hackers do?

A hacker's fundamental goal is to find a vulnerability in a system in order to manipulate the system in such a way that could cause damage. This manipulation can have a variety of effects, such as influencing vehicle functions or stealing customer data.

There are basically two types of hackers: "white hats" and "black hats." The "white hats" proactively share their findings with system owners without exploiting the vulnerability. Their work helps to accelerate the development of cybersecurity technologies and measures. This does not normally result in any damage as the company that makes the system is able to respond before the vulnerability is exploited. By contrast, the "black hats" exploit the vulnerability in a cybersecurity incident to make a profit, for example.

3) Why is cybersecurity in vehicles becoming increasingly important?

Headlines about lost data or malware attacks on computers, networks and smartphones crop up regularly in the media.

Similar to computers, tablets and smartphones, the increasing complexity of vehicles in the form of their systems, control units and applications gives rise to the threat of cyberattacks in the automotive field as well.

Connecting vehicles with other road users or transport infrastructure outside of the vehicle expands this environment.

Cybersecurity is becoming increasingly important in the context of vehicles for protecting the product and customers

4) Is there legislation on cybersecurity in the automotive sector and software updates?

The EU has recognized the importance of these topics and has applied the new UNECE Regulations No. 155 and 156 regarding cybersecurity and software updates. These regulations detail comprehensive company and certification process requirements relating to cybersecurity and software updates that vehicle manufacturers are obligated to implement.

Fulfilment of these requirements will be a prerequisite for approval of new vehicle types within the EU from mid-2022, for example.

Bentley Motors is monitoring the progress of this legislation in detail and is implementing the required measures.

5) How many known incidents affecting vehicles have there been to date?

There are no official figures as there is currently no universal system for counting incidents on either a national, international or industry level.

6) What actions is Bentley Motors taking in relation to cybersecurity?

Bentley Motors takes the cybersecurity extremely seriously to protect customers and vehicles in particular from harm. This extends from the design and development of a vehicle through to production and on to use of the vehicle by customers.

Functions are assessed for their relevance to cybersecurity and the associated risk early on in the vehicle development process and, depending on whether protection is required, corresponding protective measures are implemented in the product ("security by design"). Bentley Motors uses recognized and approved mechanisms and standards during this process and adopts state-of-the-art science and technology.

Procedures are in place during the production process to ensure that vehicles are produced in accordance with the approved design and that the software configuration process takes place in a controlled manner.

Bentley Motors continue to monitor a variety of sources to identify potential vulnerabilities or attacks, even after a vehicle has been delivered to the customer. Alongside reports from dealerships, these sources include information that is brought to our attention directly by hackers. As you would expect, data protection requirements are strictly adhered to during this monitoring.

Cross-functional teams of security experts analyse potential vulnerabilities, drawing on the knowledge of internal experts and suppliers as required.

If the analysis confirms that there is a risk to our customers or to Bentley Motors, appropriate measures to minimize the risk are initiated. These take place via established dealership processes, such as service measures, recalls or over-the-air updates on vehicles that fulfil the necessary technical requirements.

7) How are vehicles protected against attacks by hackers?

Bentley Motors take the topics of data security and vehicle security extremely seriously. A high priority is given to the implementation of security mechanisms to protect data against unauthorized access, processing, dissemination, loss, alteration or destruction in particular.

Various security mechanisms are used depending on the degree to which a particular item of data needs to be protected. In doing so we consider the security of the individual components and also the entire vehicle. Bentley Motors adopts technical and organizational protective measures that represent state-of- the-art science and technology, and uses recognized and approved mechanisms.

Examples of this are the control of data flows within the network architecture, protection against unauthorized access (e.g. use of firewalls), secured program start-up via signed software (e.g. via Secure Boot), encryption mechanisms and/or storage of sensitive data on specially secured media (e.g. using HSM hardware security model)

8) Which vehicle components are at particular risk?

Bentley Motors does not issue any general statements regarding which components are at particular risk in order to protect vehicles and in particular our customers against attackers.

Certain components are particularly attractive to hackers due to their properties (visibility, multiple interfaces, etc.).

More information about how customers can protect themselves can be found under question 12 How can I as a customer protect myself against cyberattacks when using vehicle interfaces?"

9) Is my data in the vehicle secure?

Bentley Motors takes data security extremely seriously. A high priority is given to the implementation of security mechanisms to protect data against unauthorized access, processing, dissemination, loss, alteration or destruction in particular.

Various security mechanisms are used depending on the degree to which a particular item of data needs to be protected. Bentley Motors adopts technical and organizational protective measures that represent state-of-the-art science and technology, and uses recognized and approved mechanisms.

10) How can I as a customer identify that my vehicle has been hacked?

We work on the assumption that you will generally not be able to immediately detect an attack on your vehicle. As a vehicle user, you may find that a feature does not function as expected under certain circumstances. The underlying cause can be complex. Depending on the function, it could be, for example, due to a problem in a function in the vehicle itself (e.g. screen flickering), in a Service backend (e.g. no access to services), an interface (e.g. no connection to the cellular/mobile network), etc.

If you suspect that the problem you are experiencing with the feature relates to a hacking attack, please contact your local Bentley Motor Retailer in the first instance. Give them the required information about the problem with the function. They will then conduct an analysis of the issue.

11) Who can I contact if I think that my vehicle has been hacked?

If you suspect that your vehicle has been manipulated, please contact your local Bentley Motors Retailer in the first instanc e.

The Retailer can perform an initial fault analysis on the vehicle to identify whether the cause of the abnormal behaviour of the function is due to the function itself, whether there are other causes or whether the suspicion of hacking should be pursued.

If the cause cannot be quickly identified, established communication paths between the Retailer and Bentley Motors will work in parallel to diagnose the problem.

12) How can I as a customer protect myself against cyberattacks when using vehicle interfaces?

The vehicle is equipped with a number of interfaces that you can use to connect to various devices and systems. When using these interfaces, there are measures that you can take to actively influence the protection against cyberattacks.

Wireless connections from the vehicle, e.g. Wi-Fi or Bluetooth, should be disconnected when they are not being used. In addition, passwords should be used for these connections. These passwords should contain a minimum of 12 characters, including characters from at least three of the following four categories: uppercase letters, lowercase letters, numbers, special characters. Passwords should also not be easy to guess, for example "123456" or "aaaaaa."

Only connect your own or known devices and storage media to the available interfaces such as USB or SD Card slots.

13) How should I act when handing over my vehicle?

Only give people whom you trust access to your vehicle. As soon as someone with potentially negative intentions has access to your vehicle, the possibility of manipulation that could subsequently be exploited increases.

14) Can I disable the mobile online services / My Bentley services?

You can disable the online services / My Bentley services. This disables all services that are not required by law.

You can find more information on this in the Owner's Manual for your vehicle

<u>Software updates</u>

1) How is new software installed in my vehicle and will I be informed of this?

In a Bentley Retailer, If you have a workshop appointment, the Service employee will inform you about any active software updates at the workshop reception. The update will only be installed on your vehicle if you agree to this.

If your vehicle features the required technology to receive over-the-air updates, you will be informed about any available updates for your vehicle via the infotainment system. Updates will only be installed if you actively initiate the process.

2) What influence does an update have on my vehicle?

You will always be informed about the content of the update prior to installation.

3) How frequently are features updated?

Updates are made available for your vehicle to add new functions, increase the resilience of systems or where updates are required for safety-related or legislative reasons. It is important that safety-relevant updates as well as those required by law are possible at any time to protect you, vehicle occupants and other road users. The frequency therefore depends on how necessary it is to update your vehicle.

Questionnaire Attachment to the TPI "Suspicion that control units or services have been influenced by third parties"

Model and Model Year: ____

VIN: ____

1. Where can the customer's complaint be observed?

	On the vehicle		My Bentley App		Both		Don't know

2. Describe the customer's complaint

3. Describe the sequence of actions that causes the complaint to occur

4. Do you believe there is or could be an immediate danger caused by the concern? (Immediate danger: Situation in which damage would occur or evidence lost if no action taken, e.g. endangerment of human life or sensitive customer data etc.)

	Yes		No		Unknown

Free text for explanation

5. Can you rule out the possibility that the problem was caused by misuse of a vehicle or connected service function, or a technical defect on the vehicle?

	Yes		No		Unknown

Free text for explanation

6. How often does the complaint occur?

	Constant		Daily		Weekly		Rarely

7. Has it been possible to reproduce the complaint on a comparable vehicle or version of the My Bentley App?

	Yes		No		Don’t Know

Comparable VIN	

8. How can the complaint be rectified?

	MMI Reboot		CAN Bus Sleep		Ignition cycle		Reset factory settings
	DTC Clear		App reinstall		Not possible		Other

9. When did the complaint first arise?

	Vehicle delivery		Software update		Map update
	Last workshop visit		Phone update		Other

10. Where does the complaint occur?

	Always in the same location (specify)	
	Different locations	

11. Select one data and time when the complaint occurred

Date		Time	

Space for additional relevant date(s)/time(s)

Date		Time	
Date		Time	
Date		Time	
Date		Time	

12. Please detail any equipment used by the customer that is connected to the vehicle (e.g. mobile phones using vehicle's Bluetooth/WiFi, charging cables, storage media (CD, DVD, USB etc.), devices on the OBD port, anything using the vehicle's WiFi hotspot)

13. How is the device connected to the vehicle?

	Bluetooth		WiFi		Cable		Radio Signal (e.g. vehicle key)

14. Following the customer complaints and subsequent technical investigations and diagnosis performed, do you suspect unauthorised third party influence of a control unit or service? Please explain why your response.

	Yes		No		Don't know

15. Please check the box to confirm an up-to-date full diagnostic protocol has been attached to the DISS Technical Query that this questionnaire will be attached to.

	Log attached (ID:)