Keen Security Lab Blog

2018-05-22

New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars

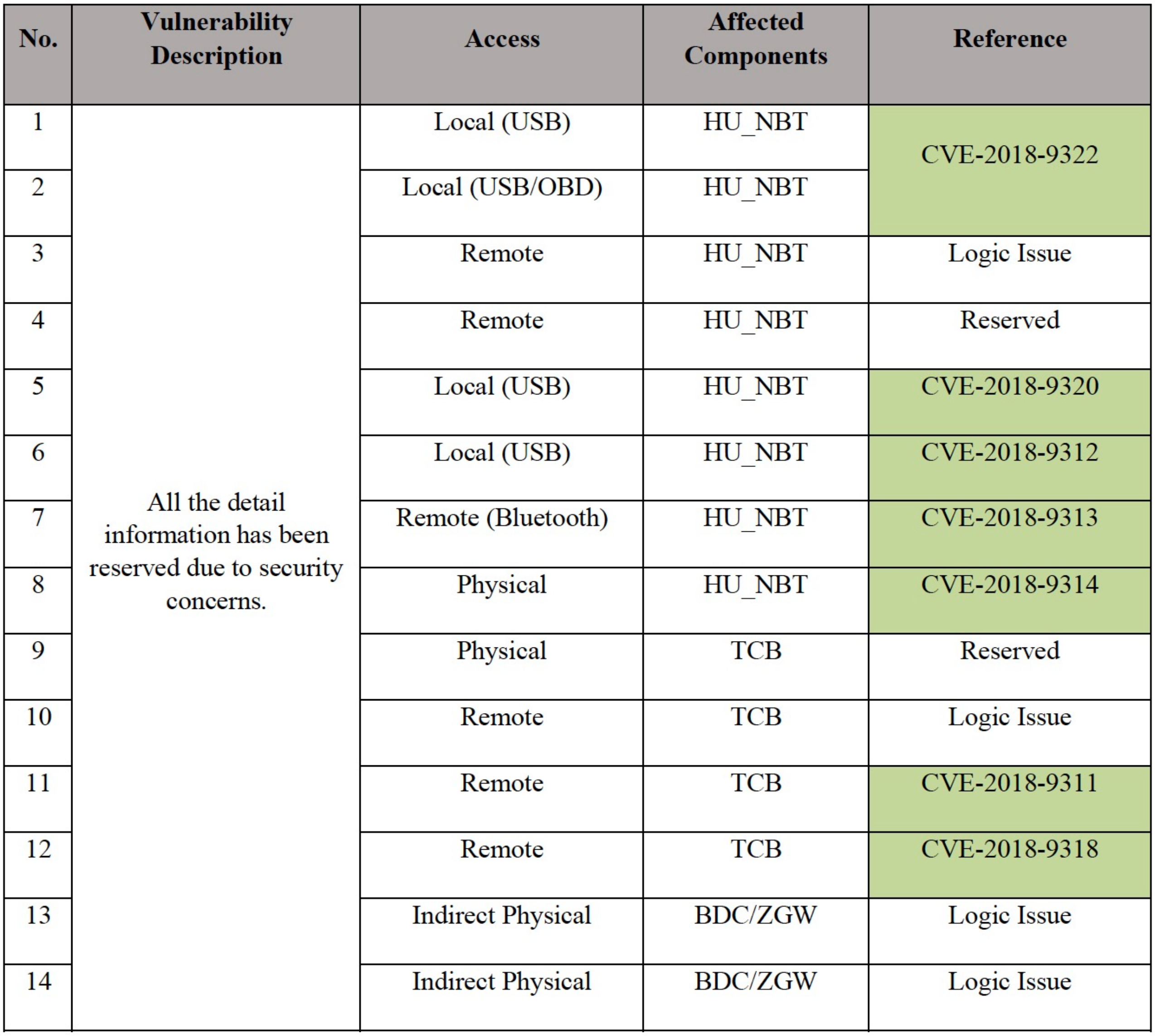
by Tencent Keen Security Lab

Introduction

The research of BMW cars is an ethical hacking research project. In the research, Keen Security Lab performed an in-depth and comprehensive analysis of both hardware and software on in-vehicle infotainment Head Unit, Telematics Control Unit and Central Gateway Module of multiple BMW vehicles. Through mainly focusing on various external attack surfaces, (including GSM network, BMW Remote Service, BMW ConnectedDrive System, Remote Diagnosis, NGTP protocol, Bluetooth protocol, USB and OBD-II interfaces), Keen Security Lab has gained local and remote access to infotainment components, T-Box components and UDS communication above certain speed of selected multiple BMW vehicle modules and been able to gain control of the CAN buses with the execution of arbitrary, unauthorized diagnostic requests of BMW in-car systems remotely.

Vulnerability Findings

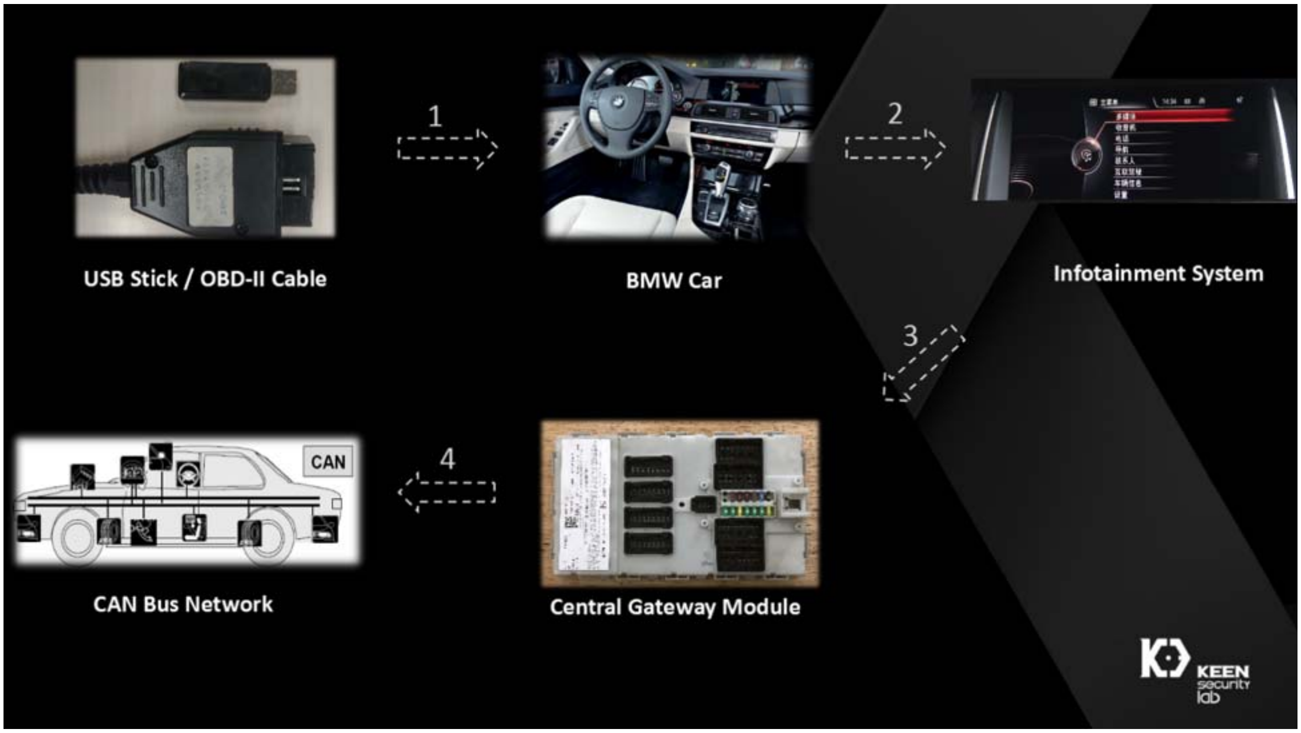
After conducting the intensive security analysis of multiple BMW cars' electronic control units, Keen Security Lab has found 14 vulnerabilities with local and remote access vectors in BMW connected cars. And 7 of these vulnerabilities were assigned CVE (Common Vulnerabilities and Exposures) numbers.
All the following vulnerabilities and CVEs have been confirmed by BMW after we submitted the full report and collaborated with them on technical details:

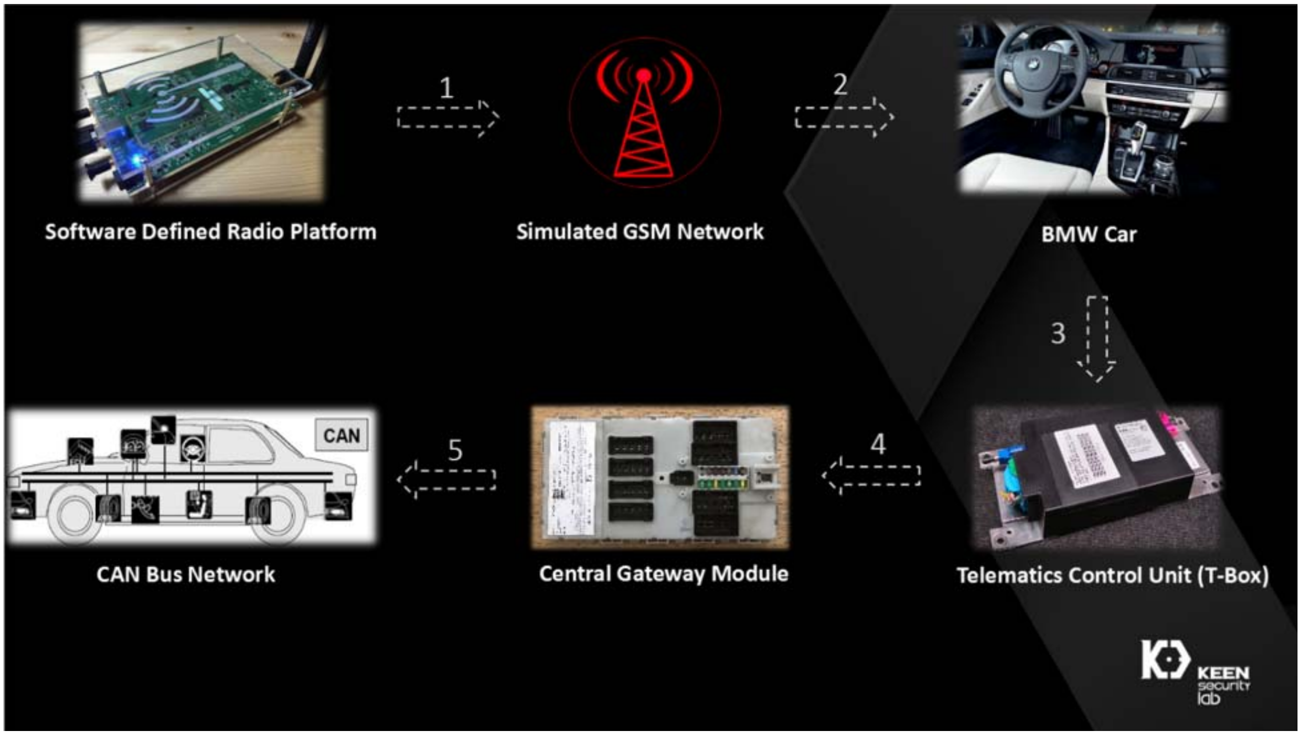


No.	Vulnerability Description	Access	Affected Components	Reference
1	All the detail information has been reserved due to security concerns.	Local (USB)	HU_NBT	CVE-2018-9322
2		Local (USB/OBD)	HU_NBT	
3		Remote	HU_NBT	Logic Issue
4		Remote	HU_NBT	Reserved
5		Local (USB)	HU_NBT	CVE-2018-9320
6		Local (USB)	HU_NBT	CVE-2018-9312
7		Remote (Bluetooth)	HU_NBT	CVE-2018-9313
8		Physical	HU_NBT	CVE-2018-9314
9		Physical	TCB	Reserved
10		Remote	TCB	Logic Issue
11		Remote	TCB	CVE-2018-9311
12		Remote	TCB	CVE-2018-9318
13		Indirect Physical	BDC/ZGW	Logic Issue
14		Indirect Physical	BDC/ZGW	Logic Issue

Attack Chains

In our research, we have already found some ways to influence the vehicle via different kinds of attack chains by sending arbitrary diagnostic messages to electronic control units. Since we were able to gain access to the head unit and telematics control unit, these attack chains are aimed to implement an arbitrary diagnostic message transmission through Central Gateway Module in order to impact or control electronic control units on different CAN buses (e.g. PT-CAN, K-CAN, etc..).

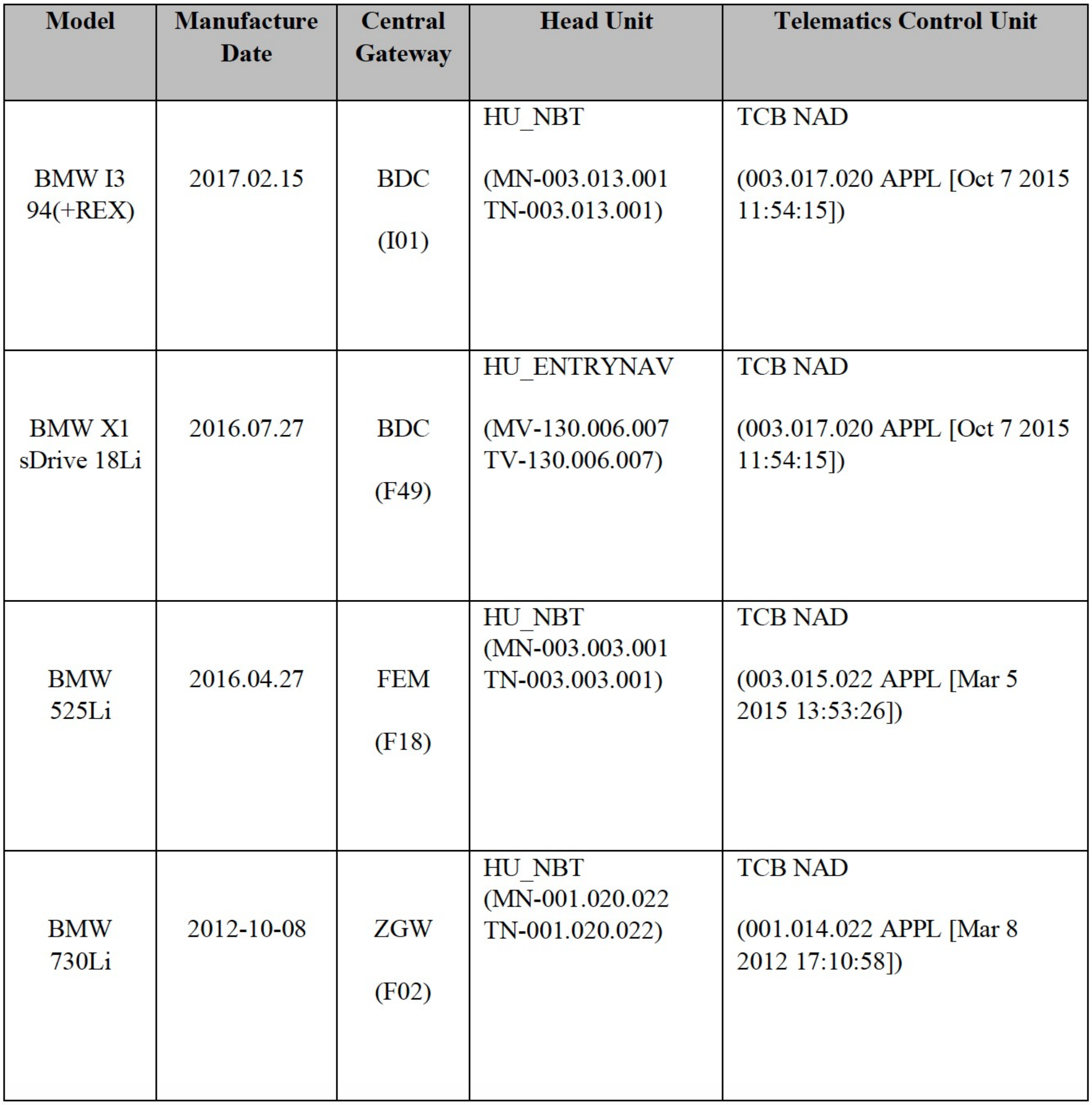




Vulnerable BMW Models

In our research, the vulnerabilities we found mainly exist in the Head Unit, Telematics Control Unit (TCB), and Central Gateway Module. Based on our research experiments, we can confirm that the vulnerabilities existed in Head Unit would affect several BMW models, including BMW i Series, BMW X Series, BMW 3 Series, BMW 5 Series, BMW 7 Series. And the vulnerabilities existed in Telematics Control Unit (TCB) would affect the BMW models which equipped with this module produced from year 2012.

Table below lists the vulnerable BMW models we’ve tested during our research and each with its firmware versions of the specific components.



Model	Manufacture Date	Central Gateway	Head Unit	Telematics Control Unit
BMW I3 94(+REX)	2017.02.15	BDC (I01)	HU_NBT (MN-003.013.001 TN-003.013.001)	TCB NAD (003.017.020 APPL [Oct 7 2015 11:54:15])
BMW X1 sDrive 18Li	2016.07.27	BDC (F49)	HU_ENTRYNAV (MV-130.006.007 TV-130.006.007)	TCB NAD (003.017.020 APPL [Oct 7 2015 11:54:15])
BMW 525Li	2016.04.27	FEM (F18)	HU_NBT (MN-003.003.001 TN-003.003.001)	TCB NAD (003.015.022 APPL [Mar 5 2015 13:53:26])
BMW 730Li	2012-10-08	ZGW (F02)	HU_NBT (MN-001.020.022 TN-001.020.022)	TCB NAD (001.014.022 APPL [Mar 8 2012 17:10:58])

As different BMW car models may be equipped with different components, and even the same component may have different firmware versions during the product lifecycle. So that from our side the scope of the vulnerable car models is hard to be precisely confirmed. Theoretically, BMW models which are equipped with these vulnerable components could be compromised from our perspective if the corrective measures had not already been effectively implemented by BMW.

BMW confirmed, that the found vulnerabilities are present in the infotainment and T-Box components mentioned above. Updates have already been developed and implemented by BMW (see below).

Disclosure Timeline

The research to BMW cars is an ethical hacking research project. Keen Lab follows the “Responsible Disclosure” practice, which is a well-recognized practice by global manufactures in software and internet industries, to work with BMW on fixing the vulnerabilities and attack chains listed in this report.

Below is the detailed disclosure timeline.

January 2017: Keen Lab kicked off the BMW security research project internally.
February 2018: Keen Lab proved all the vulnerability findings and attack chains in an experimental environment.
February 25, 2018: Keen Lab reported all the research findings to BMW.
March 9, 2018: BMW fully confirmed all the vulnerabilities reported by Keen Lab.
March 22, 2018: BMW provided the planned technical mitigation measures for the vulnerabilities reported by Keen Lab.
April 5, 2018: CVE numbers related to the vulnerabilities have been reserved. (CVE-2018-9322, CVE-2018-9320, CVE-2018-9312, CVE-2018-9313, CVE-2018-9314, CVE-2018-9311, CVE-2018-9318)
May 22, 2018: This summary report is released to public.
Early 2019: Keen Lab will release the full technical paper.

BMW informed Keen Security Lab that, for all the attacks via cellular networks BMW has started implementing measures in March 2018. These measures are in rollout since mid of April 2018 and are distributed via configuration updates remotely to the affected vehicles. Additional security enhancements are developed by BMW in form of optional SW updates. These will be available through the BMW dealer network.