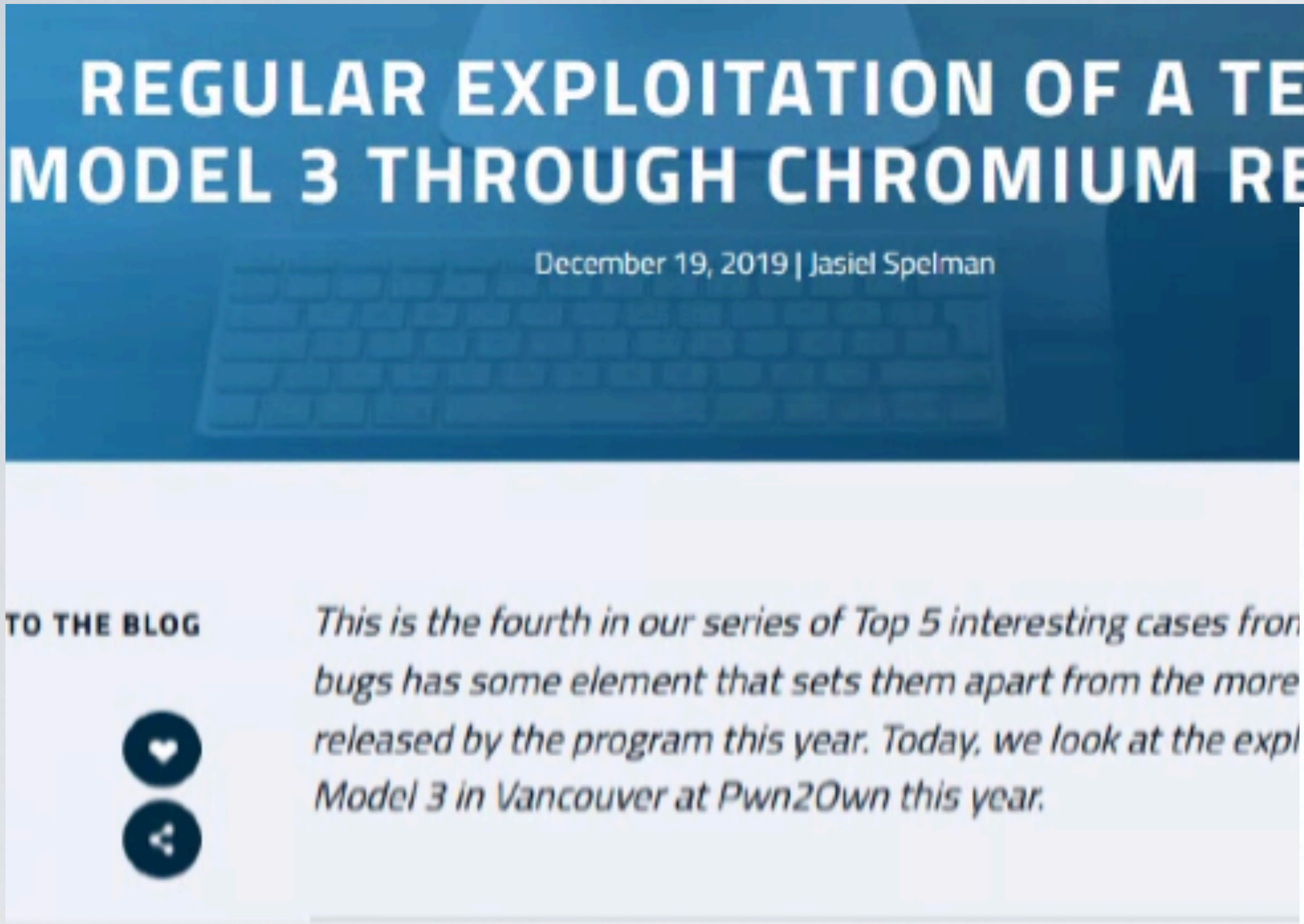


REGULAR EXPLOITATION OF A TESLA MODEL 3 THROUGH CHROMIUM REGEXP

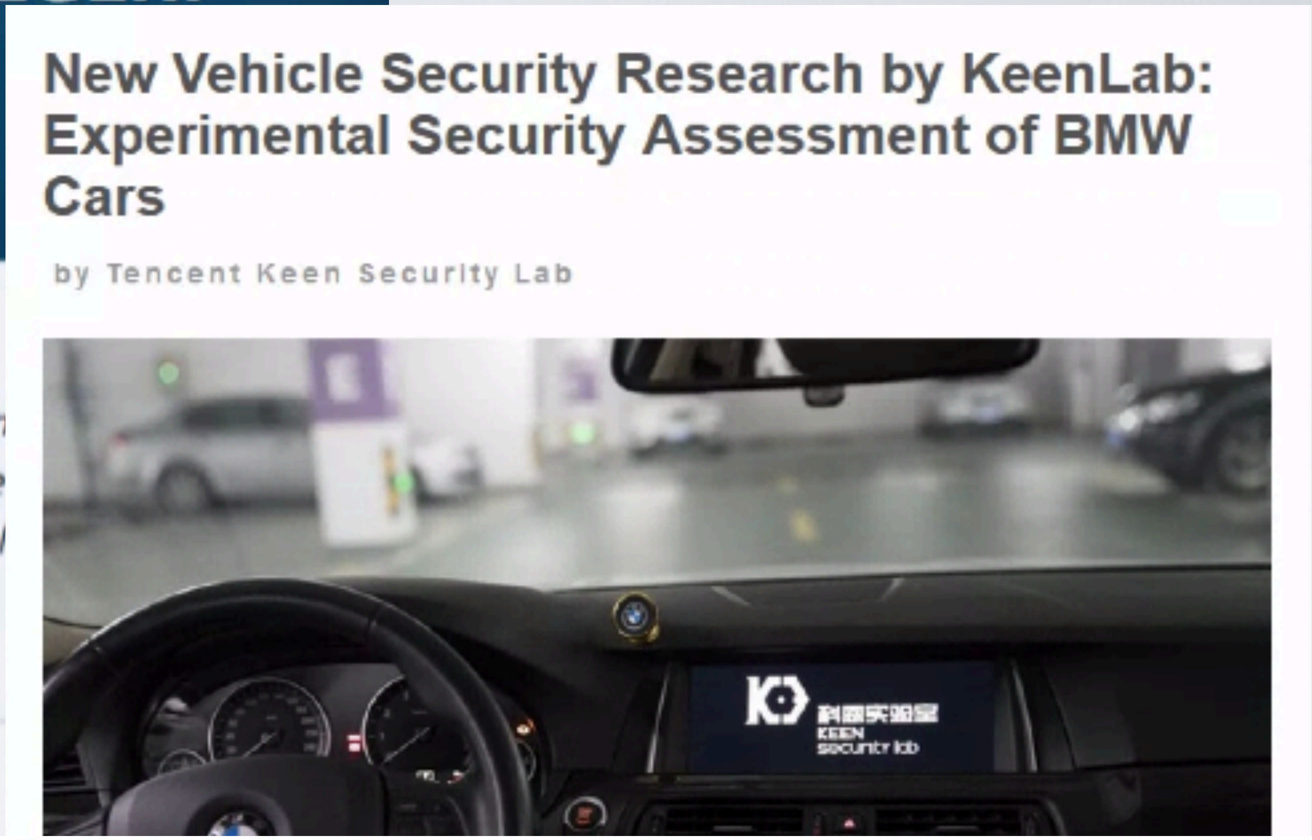
December 19, 2019 | Jasiel Spelman

TO THE BLOG

This is the fourth in our series of Top 5 interesting cases fror bugs has some element that sets them apart from the more released by the program this year. Today, we look at the expl Model 3 in Vancouver at Pwn2Own this year.

Zero Day Initiative

December 2019



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

by Tencent Keen Security Lab

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.

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.

Keen Security Lab

August 2018

Why do we have security issues?

- **Vulnerabilities**
  Memory access violations, Improper input validation …

- **Insecure configuration**
  Improper authorization, Incomplete mediation …

- **Design Weakness**
  Insufficient regard for security in system/protocol design

- **Human error**
  Careless, malicious or uninformed use of digital assets