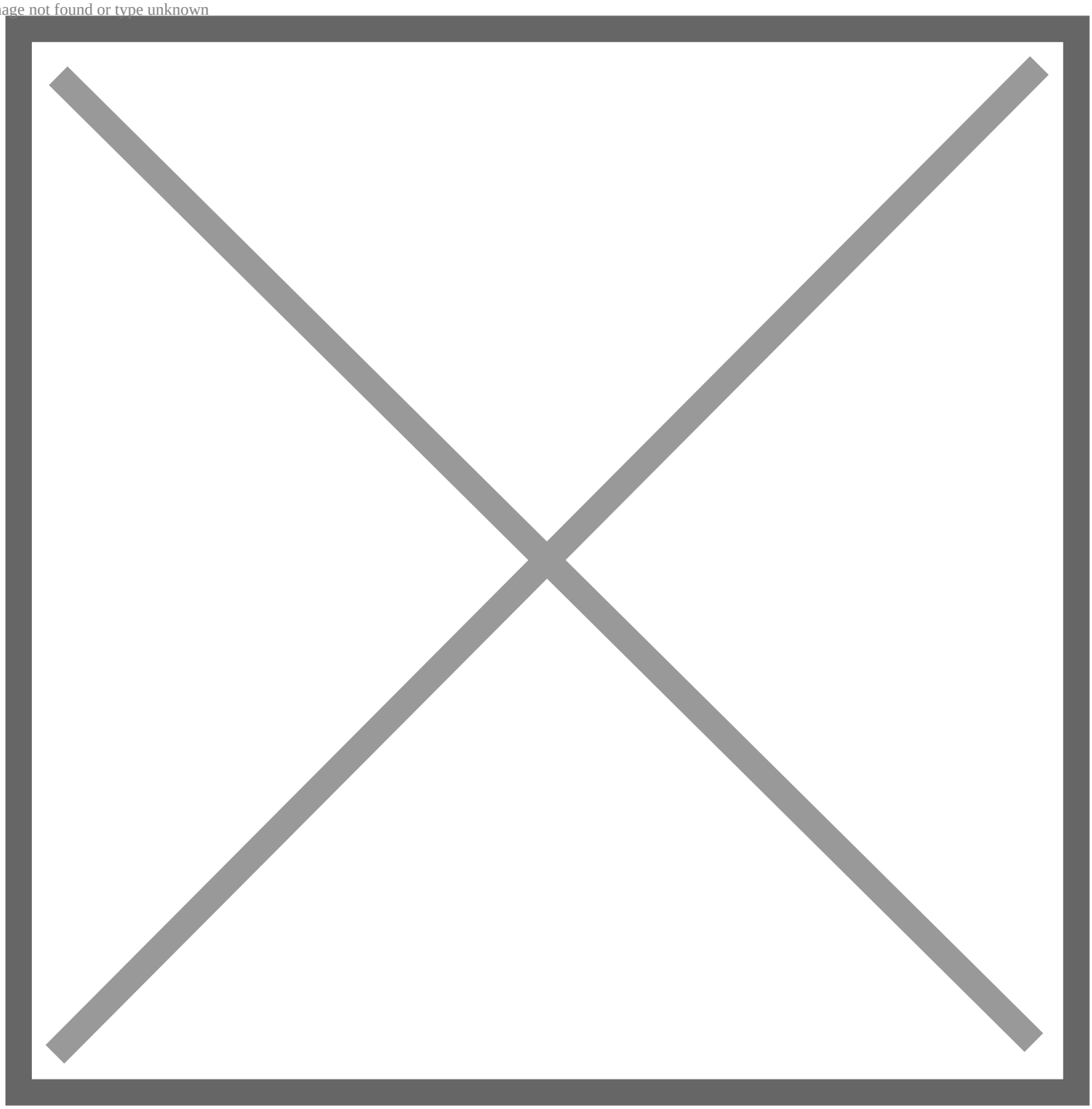
Toyota Acknowledges Tencent Keen Security Lab's Initiatives for Improving Automotive Cybersecurity

March 30, 2020

Image not found or type unknown



Vehicle performance, including the security of connected technology systems, is a top priority for Toyota. Consistent with that commitment, Toyota engages with security researchers and other vehicle manufacturers regarding vehicle and enterprise cybersecurity.

With its mission to help enhace road safety through advanced research on emerging technologies, Tencent Keen Security Lab (Keen Lab), a globally renowned cybersecurity research lab of Tencent, continues to support the strengthening of the security functions of connected vehicles by making development recommendations to automotive manufacturers.

As part of that engagement, Toyota learned from Keen Lab that they discovered vulnerabilities in certain Lexus vehicles in the market. Toyota reproduced Keen Lab's research results based on the information they provided and using the advanced scripts that they developed. Based on Toyota's investigation, operation of certain vehicle functions in certain Lexus and Toyota vehicles equipped with particular multimedia units could occur if the identified vulnerabilities in the Bluetooth function are exploited. The vulnerability findings and exploit process, as described by Keen Lab, do not control steering, braking, or throttle.

The exploitation of these vulnerabilities requires specific knowledge and expertise of the multimedia system software, a special tool, and maintaining close proximity to a vehicle for an extended period during any attempt to compromise the multimedia system. Thus, Toyota believes that exploiting these vulnerabilities in the manner developed by Keen Lab is extremely sophisticated, and the likelihood of this condition to occur in the real-world is limited.

Toyota has already implemented measures to address the vulnerabilities in the vehicles currently being produced. For certain in-market vehicles equipped with the specific multimedia units, owners can update the software by visting https://securedp.lexus.com/download-app/getUpdates (Lexus) or https://securedp.toyota.com/download-app/getUpdates (Toyota), or contacting a local Lexus or Toyota dealer.

As always, if consumers have a concern about their Toyota or Lexus vehicle, we ask they contact their local Toyota/Lexus dealer. For any additional questions, customer support is also available by calling the Toyota Customer Experience Center at 1-800-331-4331 or the Lexus Guest Experience Center at 1-800-255-3987.

Connected vehicles will play an ever-increasing role in providing safer and more secure mobility services. As connected functions become more advanced and diverse, the need for robust vehicle cybersecurity is one of the most-important issues facing the automotive industry.

With customer safety and security being a top priority, Toyota works to enhance the performance of its vehicle and enterprise cybersecurity, including by proactively conducting security testing in coordination with specialized external entities. Toyota acknowledges Keen Lab's assistance in identifying this vulnerability. Toyota takes the discovery by Keen Lab seriously and will continue to enhance the cyber protections of its vehicles.

For technical details of the Keen Lab findings, please refer to:

https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/