- Some radio security robustness issues were not identified at initial launch of connected services.
- In January 2014, through a penetration test conducted by a third party, FCA US LLC ("FCA US") identified a potential security vulnerability pertaining to certain vehicles equipped with RA3, and RA4 radios.
- A communications port was unintentionally left in an open condition allowing it to listen to and accept commands from unauthenticated sources. Additionally, the radio firewall rules were widely open by default which allowed external devices to communicate with the radio. To date, no instances related to this vulnerability have been reported or observed, except in a research setting (Miller/Valasek).
- The radio supplier began to work on security improvements immediately after the penetration testing results were known in January 2014.
- The first improvements went into production in July 2014 on 2015 MY products. Additional improvements went into production in January 2015 and July 2015, again on 2015 MY products.
- The radio supplier began developing and validating a software update for 2015 MY vehicles.
- On July 14, 2015, the FCA US' Vehicle Regulations Committee approved an extended warranty program to provide free software updates to all affected vehicle owners. FCA US did not know at that time that BU vehicles were affected.
- On June 24, 2015 the suspect period was concluded for Renegade ("BU") vehicles when the J13.4 software was introduced in production, as a product improvement.
- On July 15, 2015, FCA US held a conference call with key members of NHTSA's Research and Defect Investigation staffs to inform them of the intent to issue a TSB and customer letters.
- A follow up call was held July 17, 2015 to provide additional technical details of the condition. FCA US did not know at that time that BU vehicles were affected.
- Additionally and more importantly, the cellular carrier has remotely closed access to the open port on the radio. The cellular carrier completed a successful single market test on July 22, 2015 and a nationwide rollout on July 23, 2015. Although FCA US did not know at that time that BU vehicles were affected, the action taken by the cellular carrier to remotely close access to the open port on the radio was applied to BU vehicles. For this activity, no customer action is required and no services are interrupted. This action removes the risk of any long-range, remote hacking.
- With a large number of other vehicles with this condition being in the field for up to three years, to FCA US' knowledge there has not been a single real world incident of an unlawful or unauthorized remote hack into any FCA US vehicle.
- On July 23, 2015 FCA US determined, through the Vehicle Regulations Committee, to conduct voluntary safety recall R40 to repair all known affected vehicles.
- On August 3, 2015 FCA US confirmed that certain Jeep Renegade vehicles with the RA4 radio were also affected.
- As of August 11, 2015, FCA US has identified zero CAIRs, VOQs, and/or field reports related to this concern.
- As of August 11, 2015, total warranty is 0/1000 C's.
- As of August 11, 2015, FCA US is unaware of any accidents or injuries potentially related to this issue.