FCA US LLC Chronology
Select 2013-2015 Vehicles
RA3/4 Improved Vehicle Security Protection
Submitted on July 23, 2015

- 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 or 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.
- The supplier began to work on security improvements immediately after the penetration testing results were known in January 2014.
- Improvements that addressed closing of the open communications port and upgrades to the radio firewall were introduced to production in July 2014 on 2015 MY products. Additional improvements that addressed short range vulnerabilities were introduced to production in January 2015 and July 2015, again on 2015 MY products as a running change.
- All of these improvements were bundled into the 2013-2014 MY single service release issued in July 2015.
- On July 14, 2015, FCA US' Vehicle Regulations Committee ("VRC") approved an extended warranty program to provide free software updates to all affected vehicle owners. The committee also approved sending all affected customers an e-mail (where available) and a first class branded letter describing the importance of the software update as well as instructions of how to update their vehicles.
- The 2013-2014 MY suspect period was established as July 1, 2012 to December 1, 2014 and impacts multiple assembly plants which are as follows, Warren Truck Assembly Plant, Saltillo Truck Assembly Plant, Toledo North Assembly Plant, Connor Assembly Plant and Jefferson North Assembly Plant.
- The suspect period for 2015 MY was established as all 2015 MY Jeep Grand Cherokee, Jeep Cherokee, Dodge Durango, Dodge Viper and Ram 1500, 2500, 3500, 4500, 5500, and Chrysler 200 vehicles built prior to July 23, 2015 in U.S. markets with the sales code RA3 or RA4.
- 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 Technical Service Bulletin ("TSB") and customer letters.
- Per VRC direction and as a product improvement action, on July 16, 2015, FCA US released updated software to the field via TSB and direct customer download for all affected vehicles. Once installed, the radio will no longer default to listening and accepting commands from external sources. Additionally, the software update improves firewall rules to deny access by default to the radio.
- A follow up call was held July 17, 2015 to provide additional technical details of the condition.
- Additionally and more importantly, the cellular provider has remotely closed access to the open port on the radio. Successful single market testing was completed on July 22, 2015 with a nationwide rollout conducted on July 23, 2015. For this activity, no customer action is required and no services are interrupted. This action removes the known risk of long-range, remote hacking.
- With a large number of these vehicles 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 access into any FCA US vehicle.
- Despite the absence of any known field input, and with confirmation of remote cellular access closure eliminating all known long range risk, on July 21, 2015 NHTSA's Office of Defects Investigation requested that FCA US conduct this remedial campaign as a Safety Recall under 49 CFR 573.
- As of July 23, 2015, FCA US has identified zero CAIRs, VOQs, and/or field reports related to this concern.
- As of July 23, 2015, total warranty is 0/1000 C's.
- As of July 23, 2015, FCA US is unaware of any accidents or injuries potentially related to this issue.
- This issue was presented to the VRC on July 23, 2015. The committee decided that this security vulnerability does not constitute a Defect as defined by The Motor Vehicle Safety Act 49 USC Sec. 30102 or 49 CFR 573. The committee also decided in cooperation with NHTSA and as an abundance of caution to conduct a remedial campaign as a safety recall in the interest of protecting its customers.