U.S. Department of Transportation

National Highway Traffic Safety Administration

ODI RESUME

OFFICE OF DEFECTS INVESTIGATION
NHTSA
Authentic US Government Information
National Highway Traffic Safety Administration uses a *digital certificate* to ensure the content has remained unchanged

Investigation: RQ 15-004
Date Opened: 07/24/2015 **Date Closed:** 01/05/2016
Investigator: Kareem Habib **Reviewer:** Jeff Quandt
Approver: Stephen Ridella
Subject: Software security vulnerability

MANUFACTURER & PRODUCT INFORMATION

Manufacturer: Chrysler (FCA US LLC)
Products: MY 2013-2015 Chrysler/Dodge/Jeep/Ram with RA3 or RA4 radios
Population: 1,424,519

Problem Description: Certain vehicles equipped with Uconnect radio head units RA4 and RA3 have software security vulnerabilities which may allow unauthorized third-party access to some networked vehicle control systems.

FAILURE REPORT SUMMARY

	ODI	Manufacturer	Total
Complaints:	0	0	0
Crashes/Fires:	0	0	0
Injury Incidents:	0	0	0
Fatality Incidents:	0	0	0
Other*:	1	29	30

***Description of Other:** Malfunction allegations that appear related to other vehicle systems and components.

ACTION / SUMMARY INFORMATION

Action: This Recall Query is closed.

Summary:

On July 23, 2015, Fiat Chrysler Automobiles (FCA) launched Safety Recall 15V-461 to remedy security vulnerabilities in approximately 1.4 million model year (MY) 2013 through 2015 vehicles equipped with Uconnect head units (HU) 8.4A (RA3 radio) and 8.4AN (RA4 radio) manufactured by Harman International. On July 24, 2015, the Office of Defects Investigation (ODI) opened Recall Query, RQ 15-004, to investigate HU security vulnerabilities and remedy effectiveness in the recalled population and to determine whether similar units have been supplied for use in other FCA vehicles. In an August 11, 2015 letter, FCA submitted a second Part 573 safety recall report expanding the scope of the Uconnect RA4 model radio to include additional 7,810 MY 2015 Jeep Renegade vehicles manufactured from September 18, 2014 through June 25, 2015 (Recall 15V-508). Scope analysis indicated that Uconnect radios installed in FCA vehicles not included in recalls 15V-461 or 15V-508 (subject recalls) are not equipped with built-in cellular access or short range wireless communication features and, thus, do not contain the security vulnerabilities addressed by the subject recalls.

SUBJECT VEHICLES:
MY2014 through 2015 Dodge Durango, Jeep Grand Cherokee and Jeep Cherokee sport utility vehicles;
MY2013 through 2015 Ram 1500, 2500, 3500 and 4500/5500 pickup trucks;
MY2013 through 2015 Dodge Viper vehicles; and
MY2015 Chrysler 200, 300, Jeep Renegade, Dodge Charger and Challenger vehicles.

According to FCA, long and short range wireless vulnerabilities identified in the recalled vehicles could allow unauthorized third-party access to, and manipulation of, networked vehicle control systems. Successful exploitation of the vulnerabilities, coupled with reverse engineering of networked microprocessor control modules, could result in

unauthorized manipulation of vehicle control systems. This unauthorized manipulation of vehicle controls and systems could expose the driver, vehicle occupants or other highway users to an increased risk of injury. FCA and its network provider, Sprint, conducted a nationwide campaign to block access to a radio communications port that was unintentionally left open. On July 27, 2015, short range wireless vulnerabilities were also blocked. Finally, third party security evaluation and regression testing identified vulnerabilities that were either remedied by Sprint or through updates to the FCA Uconnect software.

ODI identified a total of 30 complaints or field reports on unique vehicles submitted by FCA (29) or received by NHTSA (1) alleging incidents of theft from a vehicle or anomalous performance that the owner alleged were caused by, or may have been caused by, remote hacking. Twenty-six (87%) of these reports were submitted after a magazine article was published on July 21, 2015, describing the remote hacking of an FCA vehicle by researchers who were able to affect the operation of various vehicle control systems, including the service brakes, steering, throttle and ignition. Most of the complaints involved vehicle systems that were not safety critical (e.g., complaints related to radio, navigation system, or air-conditioning control) and did not affect vehicle control.

Three complaints reported engine stalls. One owner reported sudden unintended acceleration allegedly related to hacking. None of the complaints or field reports reviewed involved the steering and braking vehicle control effects demonstrated by the research hackers prior to the recall. There were no confirmed incidents of hacking in any of the records reviewed by ODI. The remedies completed by Sprint and FCA appear to have eliminated vulnerabilities that might allow a remote actor to impact vehicle control systems. This recall query investigation is closed; this action does not constitute a finding by NHTSA that a safety-related defect does not exist.

(Continued on attachment A)

For additional information, see the investigative file for documents associated with this investigation. The following VOQ number is associated with the issues discussed in this closing resume: 10781035.