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
Investigator: Kareem Habib **Reviewer:** Jeff Quandt
Approver: Otto Matheke
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: 1,400,000 (Estimated)

Problem Description: Certain vehicles equipped with Uconnect 8.4AN/RA4 and 8.4A/RA3 model radios 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	TBD	TBD
Crashes/Fires:	0	TBD	TBD
Injury Incidents:	0	TBD	TBD
Number of Injuries:	0	TBD	TBD
Fatality Incidents:	0	TBD	TBD
Number of Fatalities:	0	TBD	TBD
Other*:	1	TBD	TBD

***Description of Other:** Computer security experts publicly demonstrated the ability to remotely access, modify and manipulate vehicle networks and remotely control vehicle systems. A report written by these experts documenting this was provided to NHTSA on July 20, 2015.

ACTION / SUMMARY INFORMATION

Action: Open a Recall Query.

Summary:

On July 23, 2015, Fiat Chrysler Automobiles (FCA) submitted a safety recall report to NHTSA concerning a software security defect condition in approximately 1.4 million model year (MY) 2013 through 2015 vehicles equipped with Uconnect 8.4A (RA3) and 8.4AN (RA4) radios (Recall 15V-461). According to FCA, software security vulnerabilities in the recalled vehicles could allow unauthorized third-party access to, and manipulation of, networked vehicle control systems. Manipulation of the vehicle control systems could lead to exposing the driver, the vehicle occupants or any other individual or vehicle with proximity to the affected vehicle to a potential risk of injury.

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, Dodge Charger and Challenger vehicles.

FCA indicated that access to the previously open port on the radio was remotely closed by the cellular provider on July 22, 2015, immediately eliminating any risk of long-range, illegal and unauthorized remote “hacking” for those subject vehicles accessing the cellular network. In addition, FCA will mail owners of the recalled vehicles a USB drive with a

software update that eliminates the known wireless vulnerabilities (both long and short range) for the affected vehicles. FCA made the software update available to customers for immediate installation by either directly downloading the update to their own USB drive from http://www.driveuconnect.com/software-update/ or by taking their vehicle to a dealer for immediate installation.

A Recall Query has been opened to investigate the number and models of affected vehicles, the effectiveness of the recall remedy and whether any other security vulnerabilities exist in the recalled population. ODI will also contact the manufacturer of the radio to determine whether similar units have been supplied for use in other vehicles.