

Vulnerability Note VU#819439

Fiat Chrysler Automobiles UConnect allows a vehicle to be remotely controlled

Original Release date: 24 juil. 2015 | Last revised: 27 juil. 2015

Overview

Fiat Chrysler Automobiles (FCA) UConnect may allow a remote attacker to control physical vehicle functions.

Description

According to a WIRED news article, an unknown vulnerability in FCA UConnect software allows some functions of recent models of Jeep Cherokee to be controlled by a remote attacker. Other FCA makes (including Chrysler, Dodge, and Ram) that use UConnect may also be vulnerable.

FCA with the National Highway and Transportation Safety Administration (NHTSA) has initiated a safety recall (NHTSA campaign 15V461000, "Radio Software Security Vulnerabilities") for all possibly affected makes and models:

- 2013-2015 Ram 1500 Pickup
- 2013-2015 Ram 3500 Cab Chassis
- 2013-2015 Ram 2500 Pickup
- 2013-2015 Ram 3500 Pickup
- 2013-2015 Ram 4500/5500 Cab Chassis
- 2013-2015 Dodge Viper
- 2014-2015 Jeep Cherokee
- 2014-2015 Jeep Grand Cherokee
- 2014-2015 Dodge Durango
- 2015 Chrysler 200s
- 2015 Chrysler 300s
- 2015 Dodge Challenger
- 2015 Dodge Charger

For more information, see NHTSA's report and the chronology of events leading to the recall.

It appears that some UConnect systems were configured with services listening on the Sprint mobile network. An attacker would have to have access to the Sprint mobile network.

FCA vehicles are designed with safety systems that mitigate, but do not completely prevent, this type of attack.

The paper *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, published in 2011,

documents similar research, including successful experiments gaining remote control of physical vehicle functions.

Impact

A remote attacker could control some physical functions of a vulnerable vehicle, potentially causing significant physical damage and serious or fatal injury.

The WIRED article states that the researchers were able to remotely disable the transmission, and that the car had to be stopped and restarted to restore normal operation. WIRED also reports:

Miller and Valasek's full arsenal includes functions that at lower speeds fully kill the engine, abruptly engage the brakes, or disable them altogether. The researchers say they're working on perfecting their steering control—for now they can only hijack the wheel when the Jeep is in reverse. Their hack enables surveillance too: They can track a targeted Jeep's GPS coordinates, measure its speed, and even drop pins on a map to trace its route.

Furthermore, an attacker could remotely control "...the air-conditioning, radio, and windshield wipers."

An FCA blog post states that the researchers could "...remotely controlled some functions..." but that "To FCA's knowledge, *there has not been a single real world incident of an unlawful or unauthorized remote hack* into any FCA vehicle."

Solution

Apply an update

FCA has provided an update to address this vulnerabilities, and has initiated a safety recall (NHTSA campaign 15V461000). Owners of affected models are advised to update their vehicle's UConnect software immediately. Owners can perform the update themselves or take their vehicle to a dealer to perform the update free of charge. For more information on obtaining the update or finding out if your vehicle is affected, please see FCA's news release and the recall notice at safercar.gov.

Technical Service Bulletin (TSB) 08-072-15 includes a fix for "Improved Radio security protection to reduce the potential risk of unauthorized and unlawful access to vehicle systems." The UConnect update, among other things, changes the configuration to close the listening services.

For 2013-2014 model years, update to UConnect radio version 15.26.1 or higher. For 2015 model years, update to UConnect radio version 15.17.5 or higher.

Restrict network access

Additionally, FCA provided the following statement:

FCA US has applied network-level security measures to prevent the type of remote manipulation demonstrated in a recent media report. These measures – which required no customer or dealer actions – block remote access to certain vehicle systems and were fully tested and implemented within the cellular network on July 23, 2015.

Threat modeling and secure architecture

Complex software systems contain latent vulnerabilities. Updating software to resolve vulnerabilities as they are discovered is a necessary but insufficient defensive activity. Complex, safety-critical software systems require resilient, secure design considerations.

Vehicle manufacturers should use threat models that consider skilled and potentially well-funded attackers and remote network communications. Manufacturers should also design vehicle networks to isolate or carefully limit access to safety critical systems from telematics, infotainment, diagnostic and remote communications systems.

Vendor Information [\(Learn More\)](#)

Vendor	Status	Date Notified	Date Updated
Fiat Chrysler Automobiles	Affected	-	27 Jul 2015

If you are a vendor and your product is affected, let us know.

CVSS Metrics [\(Learn More\)](#)

Group	Score	Vector
Base	8,5	AV:N/AC:M/Au:S/C:C/I:C/A:C
Temporal	6,7	E:POC/RL:OF/RC:C
Environmental	6,2	CDP:H/TD:M/CR:M/IR:H/AR:H

References

- <http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM483033/RCAK-15V461-4967.pdf>
- <http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM483036/RCLRPT-15V461-9407.pdf>
- <http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM483034/RMISC-15V461-1264.pdf>
- <http://www.safercar.gov/Vehicle+Owners>
- <http://media.fcanorthamerica.com/newsrelease.do?&id=16827&mid=1>
- http://wk2jeeps.com/tsb/tsb_wk2_0807215.pdf
- http://wk2jeeps.com/tsb/tsb_wk2_0803115a.pdf
- <http://blog.fcanorthamerica.com/2015/07/22/unhacking-the-hacked-jeep/>
- <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-15-203-01>
- <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- <http://www.wired.com/2015/07/patch-chrysler-vehicle-now-wireless-hacking-technique/>
- <http://www.driveuconnect.com/software-update/>
- <http://www.autosec.org/pubs/cars-usenixsec2011.pdf>

Credit

This vulnerability was publicly demonstrated by Charlie Miller and Chris Valasek, and initially reported by WIRED magazine. Thanks to FCA for quickly working with us to issue this vulnerability note.

This document was written by Garret Wassermann and Art Manion.

Other Information

CVE IDs: Unknown
Date Public: 21 juil. 2015
Date First Published: 24 juil. 2015
Date Last Updated: 27 juil. 2015
Document Revision: 70

Feedback

If you have feedback, comments, or additional information about this vulnerability, please send us email.