# IOActive Security Advisory

| Title | Harman-Kardon UConnect Vulnerability |
|---|---|
| Severity | Critical |
| Discovered by | Chris Valasek and Charlie Miller |
| Advisory Date | September 28, 2015 |

## Affected Product

The following UConnect 8.4AN/RA3/RA4 infotainment systems are affected:

- 2013-2015 Ram 1500/2500/3500/4500/5500
- 2013-2015 Dodge Viper
- 2014/15 Jeep Cherokee/Grand Cherokee
- 2014/15 Dodge Durango
- 2015 Chrysler 200/300
- 2015 Dodge Challenger
- 2015 Dodge Charger
- 2015 Jeep Renegade

## Impact

An attacker can remotely and without authentication compromise the affected vehicle systems.

## Background

UConnect 8.4AN/RA3/RA4 are vehicle-based infotainment systems. UConnect systems are integrated in certain makes of Chrysler, Dodge, Jeep, and Ram vehicles.

The UConnect infotainment system allowed an unauthenticated connection from other access points on the Sprint Network. An attacker could issue commands to other components within the vehicle through the infotainment system.

## Technical details

See research paper “Remote Exploitation of an Unaltered Passenger Vehicle”
http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf

## Mitigation

Sprint has disabled traffic to the vulnerable port on its network.

 

Fiat-Chrysler Automobile US (FCA US) LLC has issued a voluntary recall of 1.4 million impacted vehicles to patch the software of the UConnect Infotainment system.

## Fixes

http://www.driveuconnect.com/software-update/

http://blog.fcanorthamerica.com/2015/07/22/unhacking-the-hacked-jeep/

 