Forum:Hack Forums

Thread: Hackers Take Remote Control Of Jeep Cherokee AKA hackers took control of jeep @70 MPH

Dmitriy - *July 21, 2015, 9:24 pm*

This is an article how vulnerable the cars may be. Is the car you're driving secured? Imagine if hackers would start attacking these cars, how insane would that be?

Quote:Driving a Jeep today? Not to worry you, but unless the car has been updated in the last week, there's probably a vulnerability or two in the vehicle, as there are in as many as 471,000 Chrysler automobiles, which could be abused by hackers sitting in front of a laptop anywhere on the planet.

Wired

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Two hackers have developed a tool that can hijack a Jeep over the internet. WIRED senior writer Andy Greenberg takes the SUV for a spin on the highway while the hackers attack it from miles away.

According to researchers Chris Valasek of IOActive and Charlie Miller, a former NSA staffer, there are issues in the Uconnect system that provides the connected infotainment and other internet-powered systems in Fiat Chrysler automobiles. They were able to create attacks that could connect to that system, jump over to a chip powering the in-vehicle entertainment and rewrite the firmware on that little piece of hardware. From there, their exploit code could send commands across the car, from killing the brakes to shutting off the engine and playing with the steering, as shown in a video on Wired. It's total car compromise.

Miller and Valasek were able to connect to the Uconnect system via an Android phone running on the Sprint network (only devices using the Sprint cellular network can "speak" with Uconnect). Using that phone, hooked up to a MacBook, they were able to scan for vulnerable vehicles too. After repeated scans, they believe as many as 471,000 vehicles are carrying the vulnerabilities the benevolent hackers uncovered.

Thus far they've only tested on a Jeep Cherokee, but they believe any Chrysler vehicle with Uconnect manufactured from late 2013, all of 2014, and early 2015 is affected. The long-time car hacking buddies plan to detail their full exploits at the Blackhat security conference in two weeks' time in Las Vegas.

Pretty terrifying stuff and another example of a remote attack on a vehicle, which has been demonstrated before and will continue to be shown if car manufacturers continue to create insecure networks-on-wheels. But there is an update from Fiat Chrysler and drivers can either upload it to their vehicles by first downloading the patch onto a memory stick (via this link) and then plugging the device in, or taking it to a local dealership.

"Similar to a smartphone or tablet, vehicle software can require updates for improved security protection to reduce the potential risk of unauthorized and unlawful access to vehicle systems," read the advisory accompanying the Fiat Chrysler release.

The company had not responded to FORBES' request for comment at the time of publication, though Miller seemed satisfied with the patch.

“This is the type of vulnerability that is, or at least should be, looked out when doing a 3rd party review… That type of vulnerability isn’t specific to that Jeep and it is why it is important to have responsible disclosure policies,” noted car security expert and Open Garages founder Craig Smith.

Miller and Valasek’s findings should act as a clarion call to the whole automotive industry, which has been repeatedly criticised for shortcomings in security over the last year. Just this year, other researchers have demonstrated attacks on vehicles from afar, whilst highlighting vulnerabilities in widely-used insurance dongles that could provide leverage on a car’s network. At Defcon, a security conference taking place down the road from Blackhat in the same week, researchers also plan to show off remote attacks on a Tesla car.

Miller and Valasek have been tooting their horns about vehicular insecurities for the last two years, whilst Senator Ed Markey issued a report in February slamming major manufacturers’ response to the issue. At the same time, vehicle owners want the right to be able to hack their own cars to make modifications, but automotive manufacturers, in particular GM, want to stop that practice. In both departments, it seems they’re letting customers down.

Source

Another article: Hackers take over a Jeep driving down the highway at 70 mph
Quote:Driverless cars promise to be safer than cars driven by humans… but that’s assuming they don’t get hacked by malicious actors. Hackers Charlie Miller and Chris Valasek recently used Wired’s Andy Greenberg as a human guinea pig for their latest experiment that involved taking over his car while it was driving at a high speed.

“I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold,” Greenberg writes, in a sly reference to Hunter S. Thompson. “Though I hadn’t touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.”

Thankfully Greenberg wasn’t hurt by this attack, which he knew was coming at some point. That said, the fact that hackers figured out how to successfully pull off such an attack is fairly unnerving.

In short, Miller and Valasek have written code that can “send commands through the Jeep’s entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.” The hackers plan to give their research a full vetting at the big Black Hat conference in Las Vegas next month in what will surely be a highlight of the show.

Miller, in case you aren’t familiar with his work, has made a name for himself over the years by finding major exploits in NFC-based mobile payments technology, in Apple’s own App Store, and, yes, cars. He and Valasek started working in earnest on car hacking a couple of years ago and it seems their work has become frighteningly more advanced since then.

Source

Pretty insane, I am not surprised though. Companies trying to make the cars smarter while increasing a huge security risk. The companies need to invest more into security experts, it seems like they don't work hard enough on it. Peoples live's may be in danger.

TheNakedEmperor - *July 21, 2015, 9:25 pm*

watchdogs - real life edition

Dmitriy - *July 21, 2015, 9:26 pm*
(Jul 21, 2015 09:25 PM)TheNakedEmperor Wrote: [CITE] watchdogs - real life edition
Exactly what it seems to be. Can't imagine if there were all those gangs that would be doing that on purpose and creating drama scenes.

?Astronaut? - *July 21, 2015, 9:36 pm*
I posted a thread on Car Hacking awhile back. I thought it would be a fun project.... Looks like people are experimenting with it.

InuyashaITB - *July 21, 2015, 9:39 pm*
Seeing as how they are now implementing WIFI hotspots into vehicles, it doesn't surprise me that someone was able to infiltrate it and hook into the computers engine.
Although i find it extremely stupid that they would even implement anything external with the internal computer of the car lol.

*Side note: Don't leave your bluetooth enabled OBDii scanner plugged in :)

Dmitriy - *July 22, 2015, 8:22 pm*
I'm surprised this site is called hack forums and nobody is giving a shit about the breaches and what's being effected. What the hell is this site about then?

Bl?ckhat - *July 22, 2015, 8:31 pm*
(Jul 22, 2015 08:22 PM)Dmitriy Wrote: [CITE] I'm surprised this site is called hack forums and nobody is giving a shit about the breaches and what's being effected. What the hell is this site about then?
? Money. ?

Dmitriy - *July 22, 2015, 9:20 pm*
(Jul 22, 2015 08:31 PM)Bl?ckhat Wrote: [CITE] ? Money. ?
Guess that explains everything. That's why it's all about that market place in here lol.

emjay - *July 23, 2015, 12:05 am*
It's a cool trick, but from what I understand you need both the vin number and the car's IP. Also, there's a patch for this that takes about 2 minutes to do.

UnParad0x - *July 23, 2015, 12:07 am*
Seen this on CNN. Pretty scary shit if you ask me

Linkin™ - *July 23, 2015, 12:14 am*
Imagine if this got into the hands of terrorists, it would be absolute fucking chaos.

Dmitriy - *July 23, 2015, 12:36 am*
(Jul 23, 2015 12:14 AM)Linkin Park Wrote: [CITE] Imagine if this got into the hands of terrorists, it would be absolute fucking chaos.
That's exactly what the problem may be, just like someone can take over plane like the security researcher accomplished. It can get real nasty.
For the patching part, a lot of the people won't even know anything about it therefore will not patch their systems.

D3RP - *July 23, 2015, 1:03 am*
uh... brakes aren't connected to the vehicles entertainment system, nor are the windshield wipers.

Sorry but this isn't real.

OH GOD. I just watched the video "watch as the hackers disable the breaks so that the car slides into the ditch"... NONE of this shit is even remotely available in the stock entertainment system, they clearly are doing POC to show that the vehicle can be 3rd party chipped (connecting to ecu) to allow control of these things, such as wiring it that way. this shit is pitiful.

http://www.latimes.com/business/la-fi-jeep-cherokee-hacked-20150722-story.html

leave it to the news skids to act like any jeep 2014 etc is vulnerable to some mass hacking by some keyboard warrior.. they dont mention that the 'hacker' would have had to have internal access to your car to install their shit.

Jhawkfootball06 - *July 27, 2015, 12:21 pm*

(Jul 23, 2015 01:03 AM)D3RP Wrote: *[CITE]* uh... brakes aren't connected to the vehicles entertainment system, nor are the windshield wipers. Sorry but this isn't real.

OH GOD. I just watched the video "watch as the hackers disable the breaks so that the car slides into the ditch"... NONE of this shit is even remotely available in the stock entertainment system, they clearly are doing POC to show that the vehicle can be 3rd party chipped (connecting to ecu) to allow control of these things, such as wiring it that way. this shit is pitiful.

leave it to the news skids to act like any jeep 2014 etc is vulnerable to some mass hacking by some keyboard warrior.. they dont mention that the 'hacker' would have had to have internal access to your car to install their shit.
If you would have read the wired article, you would have found out that upon connecting to the central dashboard, they were able to override the car's firmware and install their own, giving them access to features such as control of the gas/break pedal, control of steering, control of wipers, etc. All done remotely. These cars are not equipped with a "3rd party chip" as you said.

Everything in cars nowadays is all electric, even that gas and break pedal. And they are all connected to the central CPU. That explains how services such as OnStar can remotely disable your vehicle.

Please don't belittle people's accomplishments merely because of your own ignorance.

D3RP - *July 27, 2015, 1:35 pm*

(Jul 27, 2015 12:21 PM)Jhawkfootball06 Wrote: *[CITE]* If you would have read the wired article, you would have found out that upon connecting to the central dashboard, they were able to override the car's firmware and install their own, giving them access to features such as control of the gas/break pedal, control of steering, control of wipers, etc. All done remotely. These cars are not equipped with a "3rd party chip" as you said.

Everything in cars nowadays is all electric, even that gas and break pedal. And they are all connected to the central CPU. That explains how services such as OnStar can remotely disable your vehicle.

Please don't belittle people's accomplishments merely because of your own ignorance.Excuse me.
what portion of the break pedal features a servo so that you can set a 'break 50%' command.
Same for the gas pedal. You are such a fucking sheep you will believe anything you read. Obviously you dont understand the basic mechanics behind a vehicle.
To say that the car can be remotely steered gased or braked impiles that there is a servo (as in rc toys) which applies tension to that particular mechanical MECHANISM. Im just at a loss for words

mr sheep

Not to mention that your account is 5 whole years old and you only login and post when you need to join the sheep herd

__JoeL - *July 27, 2015, 1:55 pm*
This is pretty messed up and someone would have to be pretty sadistic to mess with someone's car while they're on the highway. I could give a shit about someone's website being hacked, just being real, but for cars? That's too far.

Great Prosperity - *July 27, 2015, 7:19 pm*
This is why I will never drive an internet connected car. Or make sure to disconnect the Internet and other signals from the car.

Cars should not be integrated with the Internet. It creates unnecessary dangers. It's taking technology and putting lives at risk.

What if this was done on a massive scale by Chinese hackers. This has to stop.

CVRSE - *July 28, 2015, 4:25 pm*
shit is sketchy as balls. Fuck smart cars

Nonon Jakuzure - *July 28, 2015, 8:26 pm*
Hacking cars isn't a new concept. It's actually pretty old news. Just been hyped recently for whatever reason.
[Video: https://www.youtube.com/watch?v=3jstaBeXgAs]

Razz - *August 4, 2015, 12:24 pm*
next thing you know....fucking shit gonna be hacked and its gunna explode