NETWORK WORLD

OPEN SOURCE COMMUNITY

By Colin Neagle, Assistant Community Editor, Network World
JUL 28, 2015 1:00 PM PT

About 🔊
The Open Source subnet's hub.

With 'recall,' Fiat Chrysler makes its car hack worse

Or, how not to handle a software patch.

After Wired showed two hackers remotely gain access and immobilize a moving Jeep by exploiting software vulnerabilities last week, Fiat Chrysler responded by patching the vulnerability in several Jeep, Dodge, and Chrysler models that were equipped with the Uconnect software that was hacked. How they went about issuing the patch, however, may just put the company's customers further at risk.

Rather than simply treating the software patch as a traditional recall (i.e. requiring them to visit a service center and have an expert make the fix), Fiat Chrysler is mailing a USB thumb drive to owners of the affected cars. From there, the cars' owners can plug the USB drive into the cars' USB port to patch the software vulnerability. This seems like a convenient way to issue a recall for something that car owners can fix themselves.

However, as anybody with cybersecurity experience would well know, this opens a huge procedural window for hackers who may be inclined to exploit the vulnerability to take control of the car. Carl Leonard, principal security analyst at Raytheon Websense, says this creates an easy social engineering opportunity and uses a notoriously vulnerable distribution method in the USB drive.

"The decision of Fiat Chrysler to mail out USB sticks to customers directly to patch the recent vulnerability is the security equivalent of waving a red rag to a bull," Leonard says. "Hackers, highly adept at taking advantage of indecision and social engineering tactics in times of crisis, could potentially utilize this USB fix opportunity for nefarious gain."

For those who own these cars, attempting to patch the security vulnerability could end up backfiring if they are targeted by hackers.

"[Hackers] could, for instance, parody the update with a bogus letter and USB stick of their own, allowing them to launch a multitude of real-life threat scenarios, including crashing or stealing the car," Leonard added. "This doesn't even take into account the uncertainty that the USB patch has been applied properly without any negative consequences for the safe operation of the vehicle."

This all seems especially foolish when considering that Fiat Chrysler has also made the update available to download on its website, as well as offering service at its dealerships. So the offer to mail a pre-loaded USB device was never really necessary in the first place.

Join the Network World communities on Facebook and LinkedIn to comment on topics that are top of mind.

Colin Neagle writes about emerging technologies and the internet, among other things, and also manages Network World's blogs.

Follow 👤 ✉ 🐦 in 8⁺ 🔊

❯ **Must read: 10 new UI features coming to Windows 10**

YOU MIGHT LIKE