Interoffice Correspondence Elektros Car Co.
Palo Alto, CA

ELEKTROS

Subject	*Date*	*From*
Remote access attack	Jan. 7, 2020 12:33 PT	Petra Staeger, Senior Engineer, Electrical Systems

To: Bob Halas, Priti Prakash, Tashi Tenzing

Dear Bob, et al.

Following up on the call I had with the computer consultancy penetration testers. It's bad news.

Here's the gist of the report:

The team found a "zero-day exploit" that could target Elektros electric vehicles and give an attacker wireless control to any of our vehicles. The code enables a malicious attacker to send commands through a vehicle's environmental control systems (heat, air conditioning, etc.) to its dashboard functions, steering, brakes, and transmission. The signal could be sent from a single laptop or even a tablet or mobile phone from anywhere in the world.

This means that a hacker could kill the engine, take over steering, control turn signals, turn on/off headlights, lock the driver and passengers inside the car, and much more. They could even enable surveillance inside the car by turning on cameras or track the vehicle's location on the highway, which they could plot out on Google Maps.

Let's discuss.
Petra

Subject	*Date*	*From*
Re: Remote access attack	Jan. 7, 2020 12:41 PT	Tashi Tenzing, Engineer, Electrical Systems

To: Bob Halas, Priti Prakash, Petra Staeger

Wait, are you saying what I think you're saying? Our cars can be hacked? Is there a software solution to fix this bug?

Subject	*Date*	*From*
Remote access attack	Jan. 7, 2020 12:55 PT	Petra Staeger, Senior, Engineer, Electrical Systems

To: Bob Halas, Priti Prakash, Tashi Tenzing

Negative. Glitch is in the hardware and extends into the software. There is no short-term fix.

Subject	*Date*	*From*
Remote access attack	Jan. 7, 2020 13:50 PT	Priti Prakash, Software, Designer, Electrical Systems

To: Bob Halas, Petra Staeger, Tashi Tenzing

Holy cow!!!! Does that mean we'll have to redesign the entire hardware and electrical system from scratch? That could cost hundreds of millions of dollars and put us years behind.

Subject	*Date*	*From*
Re: Remote access attack	Jan. 7, 2020 14:46 PT	Bob Halas, Director Electrical Systems

To: Priti Prakash, Petra Staeger, Tashi Tenzing

Slow down, folks. Let me talk to the CEO. I'm sure we can come up with a plan. A lot of smart people working here. Petra, drop me the report from the pen testers.

Who else knows about this?

Subject	*Date*	*From*
Remote access attack	Jan. 7, 2020 15:13 PT	Petra Staeger, Senior Engineer, Electrical Systems

To: Bob Halas, Priti Prakash, Tashi Tenzing

Only the computer consultancy pen testers and now us. The computer nerds are bound by NDA.

Subject	*Date*	*From*
Re: Remote access attack	Jan. 7, 2020 14:46 PT	Bob Halas, Director, Electrical Systems

To: Priti Prakash, Petra Staeger, Tashi Tenzing

Good. NOBODY talk until I get some guidance from the big cheese. I mean it!!!!

Subject	*Date*	*From*
Remote access attack	Jan. 9, 2020 10:23 PT	Petra Staeger, Senior Engineer, Electrical Systems

To: Bob Halas, Priti Prakash, Tashi Tenzing

Bob,

Any word from the boss?

Subject	*Date*	*From*
Remote access attack	Jan. 10, 2020 16:49 PT	Priti Prakash, Software, Designer, Electrical Systems

To: Bob Halas, Petra Staeger, Jarrell Jameson

Bob?

Subject	*Date*	*From*
Re: Remote access attack	Jan. 13, 2020 9:46 PT	Bob Halas, Director, Electrical Systems

To: Priti Prakash, Petra Staeger, Tashi Tenzing

Hi, all:

I’ve booked conference room 74B for 2 p.m. We’ll discuss the matter then.

--