How a wireless keyboard lets hackers take full control of connected computers

reader comments

59 with 41 posters participating

Share this story

There’s a critical vulnerability in a model of Fujitsu wireless keyboard that makes it easy for hackers to take full control of connected computers, security researchers warned on Friday. Anyone using the keyboard model should strongly consider replacing it immediately.

The Fujitsu Wireless Keyboard Set LX901 uses a proprietary 2.4 GHz radio communication protocol called WirelessUSB LP from Cypress Semiconductor. While the keyboard and mouse send input that’s protected with the time-tested Advanced Encryption Standard, the USB dongle that accepts the input accepts unencrypted packets as well, as long as they’re in the proper format.

Researchers with the Germany-based penetration-testing firm SySS developed a proof-of-concept attack that exploits the insecure design. Using a small hardware device, they are able to send commands to vulnerable Fujitsu keyboard receiver dongles that are within range. As the video below demonstrates, the researchers were able to send input of their choice that’s automatically funneled to the connected computer.

[embedded content]
Fujitsu LX901 Keystroke Injection Attack PoC

But wait … it gets worse

In an advisory published Friday, the researchers warned they can combined this injection exploit with a replay attack SySS disclosed in 2016. The earlier exploit allows attackers to record encrypted keystrokes the wireless keyboard sends to the USB dongle receiver. Attackers can then launch a replay attack, in which hackers send the recorded data to the receiver. In the event hackers record the keystrokes the rightful computer owner uses to unlock the machine, the attackers can later use them to gain access when the computer is locked and unattended.

The attacks can be carried out by anyone who is within range of an affected keyboard set and takes the time to build the hardware that exploits the replay and injection flaws. Normally, that distance is about 30 feet, but the use of special antennas could extend that range. That leaves open the possibility of attacks from hackers in nearby offices or homes.

Friday's SySS advisory said that there is currently no known fix for the vulnerabilities. It said company researchers privately reported the vulnerability to Fujitsu. The disclosure timeline is:

> *2018-10-19: Vulnerability reported to manufacturer*
> *2018-10-22: Fujitsu confirms receipt of security advisory*
> *2018-10-25: Fujitsu asks for more information about the reported security issue*
> *2018-10-26: Provided more information concerning the reported security vulnerability to Fujitsu*
> *2018-10-29: Fujitsu asks for more information about the reported security issue and proof of attacks (replay and keystroke injection)*

2018-10-30: Clarified some misunderstandings concerning the replay (SYSS-2016-068) and the keystroke injection (SYSS-2018-033) vulnerabilities, provided source code of a developed PoC tool, and provided videos with proof-of-concept attacks exploiting these two security issues
2019-03-15: Public release of security advisory

Matthias Deeg, a SySS researcher, said there is no reliable way keyboard users can protect themselves against the vulnerabilities other than to ensure they are completely isolated from all other radio-based devices.

“The only protection I can think of is having an extensive control over the environment and the people where the keyboard is used,” he wrote in an email. “Using the keyboard in a radio-shielded place, for instance a basement, where no untrustworthy person can gain physical proximity and send any radio data packets to the USB receiver, should be quite secure. =).”

“But I do not recommend using this vulnerable keyboard in an environment with higher security demands,” he continued. “And I would advise not using it in exposed places where external attackers may come easily in the 2.4 GHz radio communication range of the wireless keyboard, for instance at service desks in stores, or in banks, or in train stations, or at airports.”

Attempts to reach Fujitsu representatives for comment weren’t immediately successful.

https://arstechnica.com/?p=1475021