Written by Marco Attard
18 February 2016

The connected devices making the Internet of Things (IoT) might bring more convenience, but Cisco points out major concerns with the technology-- security is not a priority among the vendors of such devices.




According to the company smart devices might make a weakest link potential hackers can exploit in order to attack home or organisation networks. Making matters worse is patching such vulnerabilities can be a complicated task, especially for non-technically savvy average user or situations where many connected devices are in use.

Cisco points out a particular vulnerable device-- the Trane ComfortLink II thermostat. Back in April 2014 Cisco's Talos security unit alerted Trane to three vulnerabilities providing a backdoor for hackers to not only gain control of the thermostat but also access networks and launch local or at-large attacks.

Eventually Trane fixed the issues (the most severe vulnerability was patched out on January 2016 via firmware version 4.0.3), and as such one should ensure customes are updated to the most recent firmware immediately. After all, very few average users even consider checking whether the software inside their smart TVs or thermostats is up to date!

Also highlighting the risks posed by connected devices is a TV show, of all things. The USA Networks series Mr. Robot has protagonist Eliot Alderson destroy the tapes inside a corporation's backup facility by hacking the HVAC system and raising the temperature. Sounds farfetched? Not so much, according to Cisco, who says customers' valuables might end up damaged if smart thermostats fail to keep temperatures at an ideal.

Either way, the lesson here is obvious-- do ensure the software running your customers' connected devices is up to date, and urge them to learn security is not an afterthought.

Go The Internet of Things is Not Always so Comforting