1030 - Hacking travel routers like it's 1999

Friday at 10:30 in Track 2
20 minutes | Demo, Exploit
Mikhail Sosonkin*Security Researcher, Synack Inc.*

Digital nomads are a growing community and they need internet safety just like anyone else. Trusted security researchers have warned about the dangers of traveling through AirBnB's. Heeding their advice, I purchased a HooToo TM06 travel router to create my own little enclave while I bounce the globe. Being a researcher myself, I did some double checking.

So, I started fuzzing and reverse engineering. While the TM06 is a cute and versatile little device - protection against network threats, it is not. In this talk, I will take you on my journey revealing my methodology for discovering and exploiting two memory corruption vulnerabilities. The vulnerabilities are severe and while they've been reported to the vendor, they are very revealing data points about the security state of such devices. While the device employs some exploitation mitigations, there are many missing. I will be showing how I was able to bypass them and what mitigations should've been employed, such as NX-Stack/Heap, canaries, etc, to prevent me from gaining arbitrary shellcode execution.

If you're interested in security of embedded/IoT systems, travel routers or just good old fashioned MIPS hacking, then this talk is for you!
Mikhail Sosonkin
Mikhail Sosonkin is a Security Researcher at Synack where he digs into the security aspects of low level systems. He enjoys automating aspects of reverse engineering and fuzzing in order to better understand application internals. Mikhail has a CS degree from NYU, where he has also taught Application Security, and a Software Engineering masters from Oxford University. Being a builder and a hacker at heart, his interests are in vulnerability analysis, automation, malware and reverse engineering. Mikhail much enjoys speaking at such conferences as ZeroNights in Moscow and DEF CON in Las Vegas!

@hexlogic, Blog http://debugtrap.com/

#defcon25/by_track/track2/friday #defcon25/By_Day/_Friday