Bug Hunting Adventures
Gotta crash them all!

Thomas Barabosch

This talk tells the story of my noble adventures as a white hat bug hunter. Throughout the last year I have found dozens of security bugs in many low-level products including AVM Fritz!OS, FreeBSD, and VirtualBox. I discuss what drove my adventures, how I hunted for bugs, and showcase some interesting cases. In addition, I reveal my toolbox (manual code reviews, fuzzing, kernel patching, ...) and explain how I utilized these techniques to quickly produce results. Another important aspect of bug hunting is (responsible) disclosure. Since this involves human communication, problems are to be expected. I give a quick overview of how to report bugs and tell the inside story of a few disclosures. After this talk, attendees will understand how white/black hat hackers may reason as well as act to find real world security vulnerabilities.