1200 - Are all BSDs are created equally? A survey of BSD kernel vulnerabilities.

Sunday at 12:00 in Track 2
45 minutes | Demo
Ilja van Sprundel*Director of penetration testing, IOActive*

In this presentation I start off asking the question "How come there are only a handful of BSD security kernel bugs advisories released every year?" and then proceed to try and look at some data from several sources. It should come as no surprise that those sources are fairly limited and somewhat outdated.

The presentation then moves on to try and collect some data ourselves. This is done by actively investigating and auditing. Code review, fuzzing, runtime testing on all 3 major BSD distributions [NetBSD/OpenBSD/FreeBSD]. This is done by first investigating what would be good places where the bugs might be. Once determined, a detailed review is performed of these places. Samples and demos will be shown.

I end the presentation with some results and conclusions. I will list what the outcome was in terms of bugs found, and who -based on the data I now have- among the 3 main BSD distributions can be seen as the clear winner and loser. I will go into detail about the code quality observed and give some pointers on how to improve some code. Lastly I will try and answer the question I set out to answer ("How come there are only a handful of BSD security kernel bugs advisories released every year?").
Ilja van Sprundel
Ilja van Sprundel is experienced in exploit development and network and application testing. As IOActive's Director of Penetration Testing, he performs primarily gray-box penetration testing engagements on mobile (specializing in iOS) and runtime (specializing in Windows kernel) applications that require customized fuzzing and source code review, identifying system vulnerabilities, and designing custom security solutions for clients in technology development telecommunications, and financial services. van Sprundel specializes in the assessment of low-level kernel code and architecture/infrastructure design, having security reviewed literally hundreds of thousands of lines of code. However, as a Director, he also functions in a managerial capacity by overseeing penetration testing engagements, providing oversight regarding technical accuracy, serving as the point of contact between technical consultants and technical stakeholders, and ensuring that engagements are delivered on time and in alignment with customer's expectations. van Sprundel also is responsible to mentor and guide Associate-level consultants as they grow both their

penetration testing and general consulting skillsets. He is the driver behind the team's implementation of cutting-edge techniques and tools, guided by both research and successful exploits performed during client engagements.

#defcon25/by_track/track2/Sunday #defcon25/By_Day/_Sunday