1300 - Demystifying Windows Kernel Exploitation by Abusing GDI Objects.

Saturday at 13:00 in 101 Track
45 minutes | Demo, Exploit
5A1F (Saif El-Sherei)*Security Analyst, SensePost*

Windows kernel exploitation is a difficult field to get into. Learning the field well enough to write your own exploits require full walkthroughs and few of those exist. This talk will do that, release two exploits and a new GDI object abuse technique.

We will provide all the detailed steps taken to develop a full privilege escalation exploit. The process includes reversing a Microsoft's patch, identifying and analyzing two bugs, developing PoCs to trigger them, turning them into code execution and then putting it all together. The result is an exploit for Windows 8.1 x64 using GDI bitmap objects and a new, previously unreleased Windows 7 SP1 x86 exploit involving the abuse of a newly discovered GDI object abuse technique.
5A1F (Saif El-Sherei)
Saif is a senior analyst with SensePost. He has a keen interest in exploit development and sharing everything he learns. Over the years he has released several exploitation tutorials, examples and a grammar-based browser fuzzer, wadi (DEF CON 23).

@saif_sherei

#defcon25/by_track/101/saturday #defcon25/By_Day/_saturday