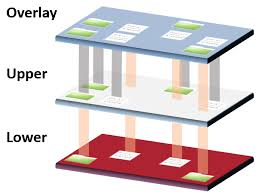
**CVE-2015-1328**

Target : Linux Kernel 3.13.0 ~ 3.19 (Ubuntu 12.04 / 14.04 / 14.10 / 15.04)와 같이 2015-06-15 이전의 kernel

Exploit Code : <https://www.exploit-db.com/exploits/37292>– Edited by C Language

Whata is it : overlayfs 사용 중 상위 파일 시스템 디렉토리에서 파일을 생성할 경우 생성 권한을 제대로 확인하지 않는 점을 통하여 local user가 root 권한으로의 상승이 가능.

OverlayFS ? overlayFS란 디렉토리 혹은 파일 시스템들을 하나의 “하위”파일 시스템으로 병합할 수 있으며 변경 내용의 경우 모두 “상위”파일 시스템에 기록할 수 있도록 하는 기능을 제공. 이와 같은 기능은 system이 read-only data를 포함하고 있으나 수정 가능한 view를 필요로 하는 Live CD나 Docker Container/Images에 유용한 기능



그림을 참조하면 알 수 있듯이 데이터를 읽어올 때는 하위 시스템으로부터 읽어오되 수정 사항이 있을 경우 이를 상위 시스템에 기록하여 원본 데이터의 손상을 최소화 할 수 있는 것으로 보임.