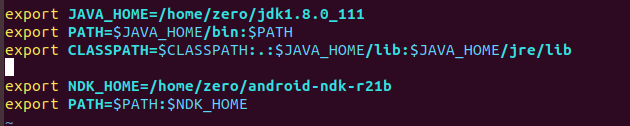
**Analyzing Android's CVE-2019-2215**

<https://dayzerosec.com/posts/analyzing-androids-cve-2019-2215-dev-binder-uaf/>

Java: <https://liquidtelecom.dl.sourceforge.net/project/wz-mle/Linux%20Tools/jdk-8u111-linux-x64.tar.gz>

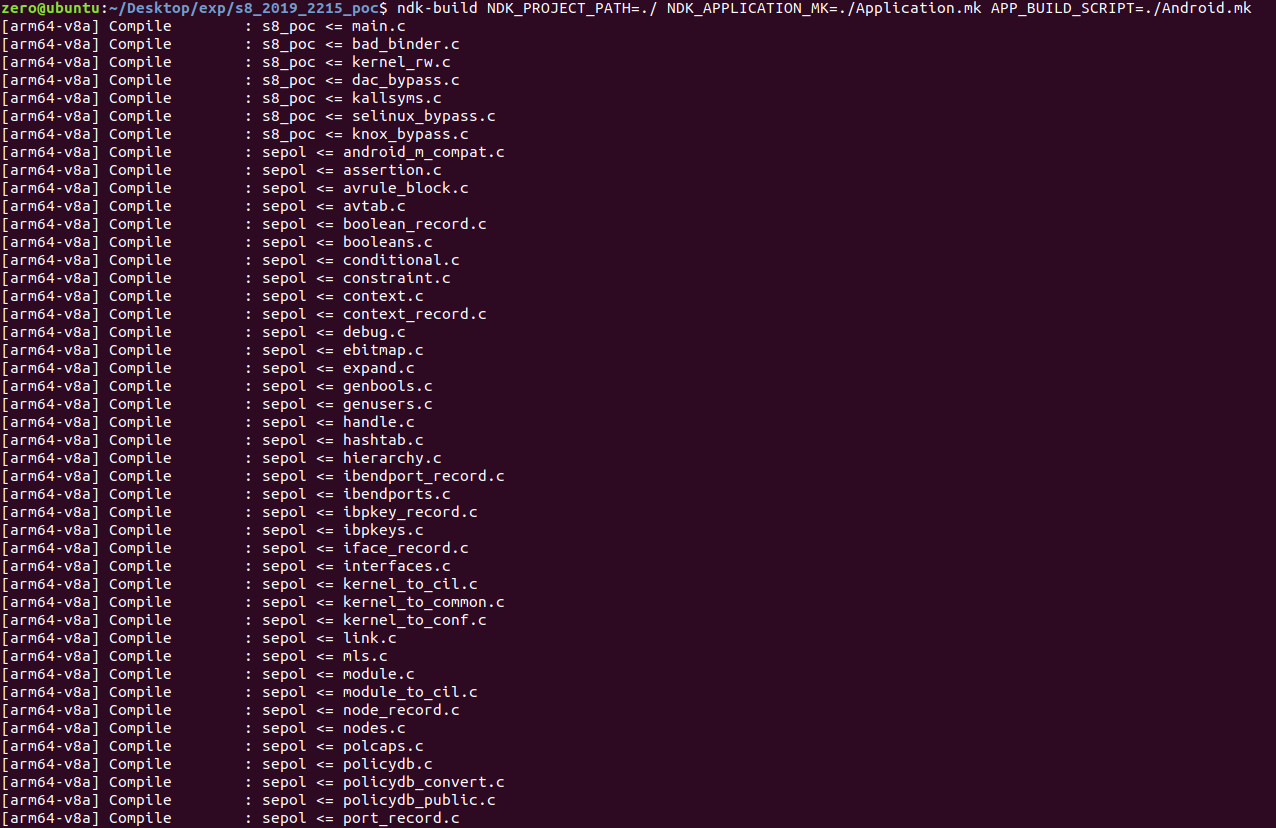
NDK: <https://dl.google.com/android/repository/android-ndk-r21b-linux-x86_64.zip>

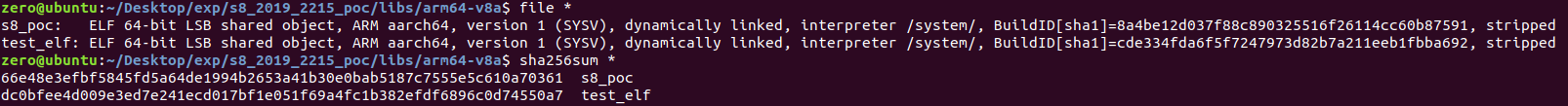
sudo vim /etc/profile



git clone [git@github.com:chompie1337/s8\_2019\_2215\_poc.git](mailto:git@github.com:chompie1337/s8_2019_2215_poc.git)

build exp：ndk-build NDK\_PROJECT\_PATH=./ NDK\_APPLICATION\_MK=./Application.mk APP\_BUILD\_SCRIPT=./Android.mk





YARA Detection:

rule AndroidOS\_CVE\_2019\_2215\_Samsung8\_EXP

{

meta:

desc = "https://github.com/chompie1337/s8\_2019\_2215\_poc/ 2019-2215 exploit for S8/S8 active with DAC + SELinux + Knox/RKP bypass"

author = "2ero"

hash = "66e48e3efbf5845fd5a64de1994b2653a41b30e0bab5187c7555e5c610a70361"

strings:

$binder = "/dev/binder" ascii wide fullword

$selinux = "/sys/fs/selinux/load" ascii wide

$avrule = "avrule\_write" ascii wide

$epoll = "epoll\_ctl" ascii wide

$readv = "readv" ascii wide

$writev = "writev" ascii wide

$waitpid = "waitpid" ascii wide

condition:

$binder and $selinux and $avrule and $epoll and $readv and $writev and $waitpid

}