Блокируем PWNKIT с помощью LSM BPF

Kernel Runtime Security Instrumentation (KRSI)

PWNKIT (CVE-2021-4034)

- Local Privilege Escalation Vulnerability in polkit’s pkexec
- CVSS v3 Base Score 7.8
- Опубликована 25 Января 2022

- pkexec установлен на многих системах, в том числе на серверах
- pkexec, suid бинарник, позволяет повышать привилегии до суперпользователя (аналог sudo)
- Если вызвать pkexec через execve без аргументов (argc == 0), то можно переписать переменную окружения GCONV_PATH и загрузить собственную разделяемую библиотеку, тем самым получив права суперпользователя без проверки

Исправление PWNKIT (CVE-2021-4034)

- В анонсе советы убрать suid бит, удалить policykit, …
- Дистрибутивы выпускают обновленную версию пакета policykit
  - нужно не забыть обновить пакет
- RedHat публикует SystemTap скрипт для блокировки pwnkit
  - Требует установки systemtap и debuginfo-install polkit на каждой машине
- Oracle для OCI выпускает runtime обновление на ядро для блокировки вызовов pkexec с argc == 0
  - нужно собирать патч для всех версий ядер
- Ariadne Conill, Kees Cook, … предлагают свой патч на ядро для блокировки execve с argc == 0
  - нужно ждать пока будет принят в апстрим, бэкпортирован на стабильные ветви, подхвачен дистрибутивами, установить пакет и перезагрузить машину
- OpenBSD хитро смотрит на это из 2015

LSM BPF

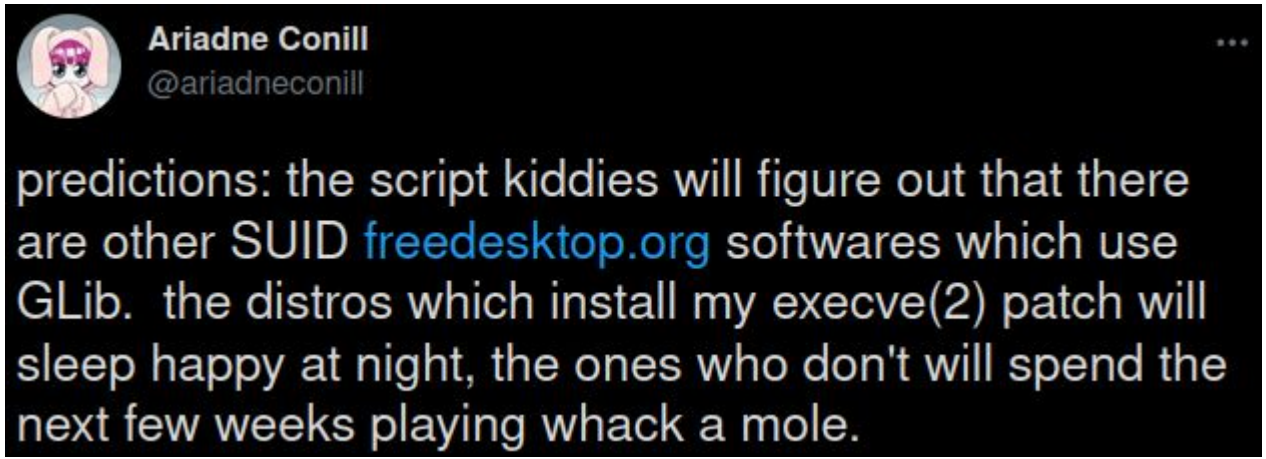
- LSM модули (SELinux, Apparmor, Smack, Tomoyo, …)
  - Мандатный контроль, контроль целостности, и другие проверки усиливающие безопасности
  - Требуют сборки вместе с ядром и загрузки вместе с ним
  - Во время обработки системных вызовов ядро спрашивает у LSM модуля можно ли продолжать
- BPF - виртуальная машина внутри ядра
- LSM BPF (KRSI)
  - В ядре с версии v5.7
  - Включается CONFIG_BPF_LSM
  - Портабельный (не требует пересборки под конкретное ядро)
  - Одновременно может работать много модулей безопасности LSM BPF

Блокируем PWNKIT с помощью LSM BPF

- Добавляется простая проверка к LSM вызову bprm_check_security
- Установить и запустить (остановить, если что-то ломает)

```
SEC("lsm/bprm_check_security")
int BPF_PROG(check_argc0, struct linux_binprm *bprm)
{
        if (bprm->argc == 0) {
                log_process_name(bprm);
                return -EINVAL;
        }

        return 0;
}
```


Ariadne Conill
@ariadneconill
predictions: the script kiddies will figure out that there are other SUID freedesktop.org softwares which use GLib. the distros which install my execve(2) patch will sleep happy at night, the ones who don't will spend the next few weeks playing whack a mole.