CVEHOUND

Ефремов Денис
efremov@linux.com

ZERONIGHTSX

Инструменты определения уязвимых версий ПО

Анализ зависимостей проекта, в большинстве случаев выполняется путем привязки к идентификатору версии уязвимой библиотеки.

- OWASP Dependency Check
- Github's Dependabot
- Snyk
- Requires.io
- Approof
- ...

DEPENDENCY-CHECK

snyk

!Requires.io

Approof

Ядро Linux. В чем сложность

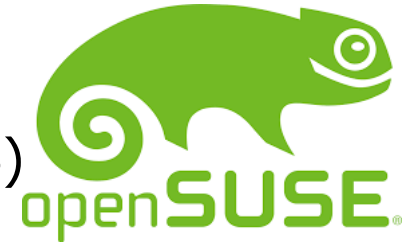
- Количество CVE
  - 1838 согласно linuxkernelcves.com (включая vendor specific)
  - 738 в базе БДУ ФСТЭК с 2014 года (не только CVE)
  - Альтернативные идентификаторы (DWF, UVI, CID, BDU, CNNVD)
- Базы неполны и неточны
  - Меньшов Виталий «Обнаружение ошибок в NVD», «Баги, которые от нас скрывают»
- Множество архитектур, тысячи CONFIG_* опций сборки
  - 17423 CONFIG_ опций в ядре 5.13
- Git история не всегда предоставляется
  - Все равно нужна разметка CVE-коммит
  - Могут быть ошибки при бэкпортировании и revert коммиты
- Стабильные ядра (LTS, XLTS) и ядра вендоров

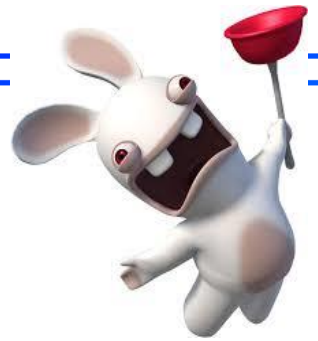
Стабильные версии

- Релиз нового ядра ~каждые 8 недель
- Стабильное ядро
  - Последнее официально выпущенное
  - На текущий момент 5.13 (5.14 в разработке)
  - На него бэкпортируются все исправления с ветки разработки 5.14
  - Следующим стабильным станет 5.14, как только будет начата разработка 5.15
- Ядра с длительным сроком поддержки (LTS 2 years, XLTS 6 years)
  - На текущий момент 5.10, 5.4, 4.19, 4.14, 4.9, 4.4
  - Минорные версии стабильного и LTS ядер релизятся ~ раз 1-2 недели
  - Чем старше ядро, тем меньше на него бэкпортируется исправлений и тем меньше оно тестируется
- Бэкпорт подразумевает что надо
  - Правильно **определить** коммит, где была внесена ошибка
  - **Корректно** портировать исправление на **все** ядра

Дистрибутивы, производители устройств

- RedHat, Canonical, Oracle (uek4), OpenSUSE, …
  - Имеют собственные стабильные версии ядер
    - 4.18 (RHEL 8), 3.10 (RHEL 7), 4.1 (UEK4), 4.15 (Bionic), 5.3 (SLES15SP3)
  - Бэкпортируют на них не только исправления, но и драйвера
  - Имеют собственные драйвера
- Civil Infrastructure Platform
  - 4.4, 4.19 Super-Long-Term-Support (SLTS 10 years)
- Samsung, Huawei, Sony, LG, OnePlus, …
  - Android Common Kernels (стабильные + android патчи)
  - У вендоров свои драйвера устройств, security драйверы,…
  - Некоторые не изменяют версию ядра при выпуске обновлений





CVEhound to the rescue

- Открыт https://github.com/evdenis/cvehound
- Не полагается на версию ядра
- Не полагается на git log
- Не требует сборки ядра
- Детекты исключительно по коду, статически
  - В диапазоне от патча с ошибкой до патча с её исправлением
  - Может определить неполные бекпорты
  - Может определить пропущенные бекпорты
- Фильтры по
  - Конфигурации сборки ядра (.config)
  - Подсистемам
  - CWE, наличию эксплоитов, …
- На текущий момент описано 212 CVE (с декабря 2020)

Примеры правил детектов CVE (шаблоны coccinelle)

CVE-2021-38166

```
@err exists@
identifier keys, values, key_size, value_size,
bucket_size;
@@

__htab_map_lookup_and_delete_batch(...) {
  ...
  keys=kvmalloc(key_size*bucket_size, ...);
  values=kvmalloc(value_size*bucket_size, ...);
  ...
}
```

CVE-2021-27363

```
@err exists@
identifier priv;
@@

show_transport_handle(...)
{
  ... when != capable(CAP_SYS_ADMIN))
  return
  \(sysfs_emit\|sprintf\)(...,
   iscsi_handle(priv->iscsi_transport));
}
```

Примеры правил детектов CVE (шаблоны coccinelle)

CVE-2021-38166

```
@err exists@
identifier keys, values, key_size, value_size,
bucket_size;
@@

__htab_map_lookup_and_delete_batch(...) {
  ...
  keys=kvmalloc(key_size*bucket_size, ...);
  values=kvmalloc(value_size*bucket_size, ...);
  ...
}
```

CVE-2021-27363

```
@err exists@
identifier priv;
@@

show_transport_handle(...)
{
  ... when != capable(CAP_SYS_ADMIN))
  return
  \(sysfs_emit\|sprintf\)(...,
   iscsi_handle(priv->iscsi_transport));
}
```

Примеры правил детектов CVE (шаблоны coccinelle)

CVE-2021-38166

```
@err exists@
identifier keys, values, key_size, value_size,
bucket_size;
@@

__htab_map_lookup_and_delete_batch(...) {
  ...
  keys=kvmalloc(key_size*bucket_size, ...);
  values=kvmalloc(value_size*bucket_size, ...);
  ...
}
```

CVE-2021-27363

```
@err exists@
identifier priv;
@@

show_transport_handle(...)
{
  ... when != capable(CAP_SYS_ADMIN))
 return
 \(sysfs_emit\|sprintf\)(...,
  iscsi_handle(priv->iscsi_transport));
}
```

Примеры правил детектов CVE (шаблоны coccinelle)

CVE-2021-38166

```
@err exists@
identifier keys, values, key_size, value_size,
bucket_size;
@@

__htab_map_lookup_and_delete_batch(...) {
  ...
  keys=kvmalloc(key_size*bucket_size, ...);
  values=kvmalloc(value_size*bucket_size, ...);
  ...
}
```

CVE-2021-27363

```
@err exists@
identifier priv;
@@

show_transport_handle(...)
{
  ... when != capable(CAP_SYS_ADMIN))
  return
  \(sysfs_emit\|sprintf\)(...,
   iscsi_handle(priv->iscsi_transport));
}
```

Примеры работы

Последнее стабильное - 4.14.244

SAMSUNG S10 (G973F) G973FXXSBFUE6

4.14.113, exynos9820-beyond1lte_defconfig

https://youtu.be/GfaVwm76NuE

HUAWEI P40 Pro+ (ELS-AN10_02_HM)

4.14.116, merge_kirin990_defconfig

https://youtu.be/hD-slpwUevI

Применение

- Исходники доступны
  - Сертификационные лаборатории для отчетов
  - Администраторы для аудита и превентивных мер
  - Разработчики для самопроверки

- Исходники недоступны
  - Запрос исходников по GPL
  - Из бинарника ядра вытащить версию ядра и архитектуру ядра
  - Из бинарника ядра вытащить .config ядра (часто доступен)
  - Проанализировать ближайшие исходники с нужной версией и конфигурацией для таргетирования

THANKS FOR ATTENTION