



CVEHOUND

Ефремов Денис
efremov@linux.com

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





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



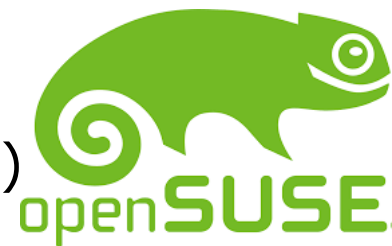
- Релиз нового ядра ~каждые 8 недель
- Стабильное ядро
 - Последнее официально выпущенное
 - На текущий момент 5.13 (5.14 в разработке)
 - На него бэкпортируются все исправления с ветки разработки 5.14
 - Следующим стабильным станет 5.14, как только будет начата разработка 5.15
- Ядра с длительным сроком 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



ORACLE®



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));
}
```

Последнее стабильное - 4.14.244

SAMSUNG S10 (G973F) G973FXXSBFUE6

4.14.113, exynos9820-
beyond1lte_defconfig

```
File Edit View Bookmarks Plugins Settings Help
CVSS2: 4.9
CVSS3: 5.5
FIX DATE: 2020-11-07 12:07:26
https://www.linuxkernelcves.com/cves/CVE-2020-25704
Affected Files:
- ./kernel/events/core.c: CONFIG_PERF_EVENTS

Found: CVE-2020-27068
MSG: cfb80211: add missing policy for NL80211_ATTR_STATUS_CODE
CWE: Out-of-bounds Read
CVSS2: 2.1
CVSS3: 4.4
FIX DATE: 2020-02-14 08:50:37
https://www.linuxkernelcves.com/cves/CVE-2020-27068
Affected Files:
- ./net/wireless/nl80211.c: CONFIG_CFG80211 & CONFIG_WIRELESS

Found: CVE-2020-27825
MSG: trace: ring_buffer: add missing policy for TRACE_RING_BUFFER
CWE: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CVSS2: 4.4
CVSS3: 5.7
FIX DATE: 2020-10-15 16:01:13
https://www.linuxkernelcves.com/cves/CVE-2020-27825
Affected Files:
- ./kernel/trace/ring_buffer.c: CONFIG_RING_BUFFER

Found: CVE-2020-29370
MSG: mm: slub: add missing IID bump in kmem_cache_alloc_bulk()
CWE: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CVSS2: 4.4
CVSS3: 7.0
FIX DATE: 2020-03-18 16:21:51
https://www.linuxkernelcves.com/cves/CVE-2020-29370
Affected Files:
- ./mm/slub.c: CONFIG_SLUB
```

Примеры работы

HUAWEI P40 Pro+ (ELS- AN10_02_HM)

4.14.116,
merge_kirin990_defconfig

```
File Edit View Bookmarks Plugins Settings Help
FIX DATE: 2020-02-20 10:03:14
https://www.linuxkernelcves.com/cves/CVE-2020-9391
Affected Files:
- ./mm/mmap.c: CONFIG_MMU
- ./mm/mremap.c: CONFIG_MMU

Found: CVE-2021-0512
MSG: HID: make arrays usage and value to be the same
CWE: Out-of-bounds Write
CVSS2: 4.6
CVSS3: 7.8
FIX DATE: 2021-01-18 08:09:57
https://www.linuxkernelcves.com/cves/CVE-2021-0512
Affected Files:
- ./drivers/hid/hid-core.c: CONFIG_HID

Found: CVE-2021-0605
MSG: af_key: pfkey_dump needs parameter validation
CWE: Out-of-bounds Read
CVSS2: 4.9
CVSS3: 4.4
FIX DATE: 2020-07-22 16:04:22
https://www.linuxkernelcves.com/cves/CVE-2021-0605
Affected Files:
- ./net/key/af_key.c: CONFIG_NET_KEY

Found: CVE-2021-33909
MSG: seq_file: disallow extremely large seq buffer allocations
CWE: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CVSS2: 7.2
CVSS3: 7.8
FIX DATE: 2021-07-20 00:18:48
https://www.linuxkernelcves.com/cves/CVE-2021-33909
Affected Files:
- ./fs/seq_file.c: True
```

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

