Форум ITSEC 2025
17-18 июня

Доверенный open-source в корпоративном репозитории

Алексей Хорошилов
khoroshilov@ispras.ru

ИСП РАН
Институт системного программирования им. В.П. Иванникова
Российской академии наук

Доверенный open-source

- ✗ Цепочки поставок
- ✗ Среда сборки
- ✗ Собственный код

Доверенный open-source в корпоративном репозитории

- ✗ Цепочки поставок
- ✗ Среда сборки
- ✗ Собственный код

- ✗ Доверенный open-source в бинарном виде

Доверенный open-source

Доверенный open-source

- Заимствованное доверие
  - звёзды на github
  - используется в ...

Доверенный open-source

- Заимствованное доверие
  - звёзды на github
  - используется в ...

в корпоративном репозитории

- Контроль полноты
- Контроль устранения уязвимостей
- Контроль, что в репозитории тоже, что и у заёмодателя

Доверенный open-source

Доверенный open-source

- Доверие к программам добровольной оценки зрелости
  - https://www.bestpractices.dev/ru/criteria

OpenSSF Best Practices

OpenSSF Best Practices

OpenSSF Best Practices

- Основы
  - Основная информация на веб-сайте проекта
  - Свободная лицензия
  - Документация
  - Другое
- Управление изменениями
  - Публичное хранилище исходного кода с поддержкой версий
  - Уникальная нумерация версий
  - Примечания к выпуску
- Отчеты о проблемах
  - Процесс сообщения об ошибках
  - Процесс отчетов об уязвимостях
- Качество
  - Рабочая система сборки
  - Набор автотестов
  - Тестирование новых функций
  - Флаги предупреждений
- Безопасность
  - Знание безопасной разработки
  - Основы правильного использования криптографии
  - Доставка, защищенная от атак посредника (MITM)
  - Исправление обнародованных уязвимостей
  - Другие вопросы безопасности
- Анализ
  - Статический анализ кода
  - Динамический анализ кода

Доверенный open-source

- Контролируемое доверие
  - Воспроизведение
    - сборки/статического анализа
    - тестов
    - фаззинг-тестирования

Доверенный open-source

- Контролируемое доверие
  - Воспроизведение
    - сборки/статического анализа
    - тестов
    - фаззинг-тестирования
  - Развитие
    - дополнительный статический анализ
    - дополнительные тесты
    - новые фаззинг-цели

Центр исследований безопасности системного ПО

https://portal.linuxtesting.ru
https://gitlab.community.ispras.ru/cc-portal/intro

У каждого проекта – своя специфика РБПО и своё сообщество

599

патчей принято в исходный код ядра

197

патчей принято в исходный код компонентов

Сейчас в работе

Ядро Linux 35 млн строк
NGinx 0,2 млн строк
OpenSSL 0,9 млн строк
Виртуализация
- **Qemu 1,6 млн строк**
- **spice-server 75 тыс. строк**
- **Usbredir 10 тыс. строк**
- **libvirt 1,6 млн строк**
- **Podman 0,4 млн строк**

Python
- **CPython 1,6 млн строк**
- **PyYAML 10 тыс. строк**

Node.JS 7 млн строк
.NET
- **.NET Runtime 8,3 млн строк**
- **ASP.NET Core 1,1 млн строк**
- **NewtonSoft.Json 135 тыс. строк**
- **SharpCompress 80 тыс. строк**

>70

организаций ведут совместную работу

АКТИВ, ареал консалтинг, АТЛАС научно-технический центр, СФБ ЛАБ, ГАРДА технологии, ЭЗТ ЗАО "Защита электронных технологий", САФИБ, kaspersky, НПЦ КСБ, INFOWATCH, R-Vision

Ядро Linux

- 35+ млн. строк кода
  - регулярный выпуск версии раз в 2-2,5 месяца
  - более 1600 разработчиков в каждой версии
  - ~7 изменения (коммита) каждый час
  - ~4 тыс. строк кода добавляется каждый день
  - ~1.5 тыс. строк кода изменяется каждый день
  - ~1.5 тыс. строк кода удаляется каждый день
  - стабильные ветки с бэкпортированием 50ё0+ исправлений в месяц
  - CVE Numbering Authority (200-600 CVE в месяц)

(*) по статистике за 15 лет: 2010-2025

Примеры результатов анализа

[АНОНС] Релиз ядра linux-5.10.236-lvc50	Alexey Khoroshilov	25.04.2025, 09:37
[АНОНС] Релиз ядра linux-6.1.134-lvc22	Alexey Khoroshilov	25.04.2025, 11:06
[АНОНС] Кандидат на релиз ядра linux-5.10.236-lvc51-rc1	Alexey Khoroshilov	28.04.2025, 14:36
[АНОНС] Кандидат на релиз ядра linux-6.1.135-lvc23-rc1	Alexey Khoroshilov	29.04.2025, 13:36
[АНОНС] Релиз ядра linux-5.10.236-lvc51	Alexey Khoroshilov	03.05.2025, 17:11
[АНОНС] Релиз ядра linux-6.1.135-lvc23	Alexey Khoroshilov	03.05.2025, 17:58
[АНОНС] Кандидат на релиз ядра linux-6.1.136-lvc24-rc1	Alexey Khoroshilov	04.05.2025, 20:38
[АНОНС] Кандидат на релиз ядра linux-5.10.237-lvc52-rc1	Alexey Khoroshilov	05.05.2025, 09:58
[АНОНС] Кандидат на релиз ядра linux-5.10.237-lvc52-rc2	Alexey Khoroshilov	07.05.2025, 09:39
[АНОНС] Кандидат на релиз ядра linux-6.1.137-lvc24-rc2	Alexey Khoroshilov	07.05.2025, 11:18
[АНОНС] Релиз ядра linux-5.10.237-lvc52	Alexey Khoroshilov	12.05.2025, 09:55
[АНОНС] Релиз ядра linux-6.1.137-lvc24	Alexey Khoroshilov	12.05.2025, 09:57
[АНОНС] Кандидат на релиз ядра linux-5.10.237-lvc53-rc1	Alexey Khoroshilov	19.05.2025, 11:12
[АНОНС] Кандидат на релиз ядра linux-6.1.139-lvc25-rc1	Alexey Khoroshilov	19.05.2025, 14:45
[АНОНС] Релиз ядра linux-5.10.237-lvc53	Alexey Khoroshilov	22.05.2025, 13:26
[АНОНС] Кандидат на релиз ядра linux-6.1.139-lvc25-rc2	Alexey Khoroshilov	22.05.2025, 14:27
[АНОНС] Релиз ядра linux-6.1.139-lvc25	Alexey Khoroshilov	29.05.2025, 20:12
[АНОНС] Кандидат на релиз ядра linux-5.10.237-lvc54-rc1	Alexey Khoroshilov	04.06.2025, 12:07
[АНОНС] Кандидат на релиз ядра linux-6.1.140-lvc26-rc1	Alexey Khoroshilov	04.06.2025, 15:00
[АНОНС] Релиз ядра linux-5.10.237-lvc54	Alexey Khoroshilov	07.06.2025, 16:24
[АНОНС] Релиз ядра linux-6.1.140-lvc26	Alexey Khoroshilov	07.06.2025, 20:33
[АНОНС] Кандидат на релиз ядра linux-6.1.141-lvc27-rc1	Alexey Khoroshilov	13.06.2025, 00:43
[АНОНС] Кандидат на релиз ядра linux-5.10.238-lvc55-rc1	Alexey Khoroshilov	13.06.2025, 14:08
[АНОНС] Кандидат на релиз ядра linux-6.1.141-lvc27-rc2	Alexey Khoroshilov	17.06.2025, 21:30
[АНОНС] Кандидат на релиз ядра linux-5.10.238-lvc55-rc2	Alexey Khoroshilov	17.06.2025, 21:33

Ведение собственных веток ядра (1)

[АНОНС] Релиз ядра linux-5.10.237-lvc52

Опубликован релиз ядра linux-5.10.237-lvc52 [1], в котором:
1. В качестве базовой версии ядра Linux используется версия 5.10.237 (вместо 5.10.236), что включает в себя исправления следующих уязвимостей:
- BDU:2024-04220 (CVE-2024-35867) "smb: client: fix potential UAF in cifs_stats_proc_show()" (Уровень опасности 7.8)
- BDU:2025-04678 (CVE-2023-52757) "smb: client: fix potential deadlock when releasing mids" (Уровень опасности 7.8)
- BDU:2024-01940 (CVE-2023-52572) "cifs: Fix UAF in cifs_demultiplex_thread()" (Уровень опасности 7.8)
- BDU:2024-03668 (CVE-2024-26928) "smb: client: fix potential UAF in cifs_debug_files_proc_show()" (Уровень опасности 7.8)
- CVE-2025-37838 "HSI: ssi_protocol: Fix use after free vulnerability in ssi_protocol Driver Due to Race Condition" (Уровень опасности 7.8)
- CVE-2021-47247 "net/mlx5e: Fix use-after-free of encap entry in neigh update handler" (Уровень опасности 7.8)
- CVE-2023-52621 "bpf: Check rcu_read_lock_trace_held() before calling bpf map helpers" (Уровень опасности 7.8)
- CVE-2024-36908 "blk-iocost: do not WARN if iocg was already offlined" (Уровень опасности 7.1)
- CVE-2024-46774 "powerpc/rtas: Prevent Spectre v1 gadget construction in sys_rtas()" (Уровень опасности 7.1)
- BDU:2025-03473 (CVE-2024-50154) "tcp/dccp: Don't use timer_pending() in reqsk_queue_unlink()." (Уровень опасности 7.0)
- BDU:2025-01478 (CVE-2025-21681) "openvswitch: fix lockup on tx to unregistering netdev with carrier" (Уровень опасности 5.5)
- BDU:2023-01211 (CVE-2023-23000) "phy: tegra: xusb: Fix return value of tegra_xusb_find_port_node function" (Уровень опасности 5.5)
- BDU:2024-09857 (CVE-2024-27054) "s390/dasd: fix double module refcount decrement" (Уровень опасности 5.5)
- CVE-2022-49309 "drivers: staging: rtl8723bs: Fix deadlock in rtw_surveydone_event_callback()" (Уровень опасности 5.5)
- CVE-2024-26686 "fs/proc: do_task_stat: use sig->stats_lock to gather the threads/children stats" (Уровень опасности 5.5)
- CVE-2022-48893 "drm/i915/gt: Cleanup partial engine discovery failures" (Уровень опасности 5.5)
- CVE-2022-49190 "kernel/resource: fix kfree() of bootmem memory again" (Уровень опасности 5.5)
- CVE-2025-21853 "bpf: avoid holding freeze_mutex during mmap operation" (Уровень опасности 5.5)

Ведение собственных веток ядра (2)

[АНОНС] Релиз ядра linux-5.10.237-lvc52

Опубликован релиз ядра linux-5.10.237-lvc52 [1], в котором:
…
2. Добавлен патч "net: hns3: add vlan list lock to protect vlan list" (Jian Shen <shenjian15@huawei.com>, бэкпортирован Dmitry Antipov <dmantipov@yandex.ru>), устраняющий уязвимость CVE-2022-49182 (Уровень опасности 7.8).
3. Добавлен патч "ext4: fix uninitialized value in ext4_mb_init_cache()" (Igor.A.Artemiev@mcst.ru), устраняющий ошибки:
- VARIABLE_IS_NOT_ARRAY: fs/ext4/mballoc.c:1233
- VARIABLE_IS_NOT_ARRAY: fs/ext4/mballoc.c:1235
4. Добавлен патч "lib/cmdline: avoid page fault in next_arg" (Neel Natu <neelnatu@google.com>, бэкпортирован Igor Artemiev <Igor.A.Artemiev@mcst.ru>), устраняющий ошибку "INTEGER_OVERFLOW: lib/cmdline.c:238".
5. Добавлен патч "mac80211: aes_cmac: check crypto_shash_setkey() return value" (Johannes Berg <johannes.berg@intel.com>, бэкпортирован Igor Artemiev <Igor.A.Artemiev@mcst.ru>), устраняющий ошибку "UNCHECKED_FUNC_RES.STAT: net/mac80211/aes_cmac.c:77".
6. Добавлен патч "staging: r8188eu: Fix possible NULL dereference" (Murad Masimov <m.masimov@maxima.ru>, бэкпортирован Igor Artemiev <Igor.A.Artemiev@mcst.ru>), устраняющий ошибку "DEREF_OF_NULL.RET.STAT: drivers/staging/rtl8188eu/os_dep/recv_linux.c:115".
7. Добавлен патч "leds: uleds: fix unchecked copy_to_user() in uleds_read()" (Ivan Stepchenko <sid@itb.spb.ru>), устраняющий ошибку "UNCHECKED_FUNC_RES.STAT: drivers/leds/uleds.c:150".
8. Добавлен патч "usb: gadget: composite: fix possible kernel oops in composite_setup()" (Sergey Shtylyov <s.shtylyov@omp.ru>), устраняющий ошибки:
- REDUNDANT_COMPARISON.ALWAYS_FALSE: drivers/usb/gadget/composite.c:1860
- UNREACHABLE_CODE: drivers/usb/gadget/composite.c:1861
9. Добавлена серия патчей
- "cifs: fix session state transition to avoid use-after-free issue" (Winston Wen <wentao@uniontech.com>, бэкпортирован Fedor Pchelkin <pchelkin@ispras.ru>)

Ведение собственных веток ядра (3)

[АНОНС] Релиз ядра linux-5.10.237-lvc52 от 12 мая 2025

Опубликован релиз ядра linux-5.10.237-lvc52 [1], в котором:
…
В базовую версию ядра 5.10.237 также вошли исправления уязвимостей, которые уже были устранены в lvc-ветках:
- CVE-2025-37782 "hfs/hfsplus: fix slab-out-of-bounds in hfs_bnode_read_key" - была устранена в linux-5.10.232-lvc40 от 31 декабря 2024 года (Vasiliy Kovalev <kovalev@altlinux.org>)
- BDU:2024-09005 (CVE-2024-49960) "ext4: fix timer use-after-free on failed mount" (Уровень опасности 7.8) - была устранена в linux-5.10.233-lvc41 от 20 января 2025 года (Xiaxi Shen <shenxiaxi26@gmail.com>, бэкпортирован Dmitriy Privalov <d.privalov@omp.ru>)
- BDU:2024-04576 (CVE-2023-52752) "smb: client: fix use-after-free bug in cifs_debug_data_proc_show()" (Уровень опасности 7.8) - была устранена в linux-5.10.233-lvc41 от 20 января 2025 года (Paulo Alcantara <pc@manguebit.com>, бэкпортирован Dmitriy Privalov <d.privalov@omp.ru>)
- BDU:2024-08315 (CVE-2024-41073) "nvme: avoid double free special payload" (Уровень опасности 7.8) - была устранена в linux-5.10.233-lvc41 от 20 января 2025 года (Chunguang Xu <chunguang.xu@shopee.com>, бэкпортирован Dmitriy Privalov <d.privalov@omp.ru>)
- BDU:2025-04676 (CVE-2024-56658) "net: defer final 'struct net' free in netns dismantle" (Уровень опасности 7.8) - была устранена в linux-5.10.234-lvc43 от 16 февраля 2025 года (Eric Dumazet <edumazet@google.com>, бэкпортирован Vasiliy Kovalev <kovalev@altlinux.org>)
- BDU:2024-09012 (CVE-2024-50047) "smb: client: fix UAF in async decryption" (Уровень опасности 7.8) - была устранена в linux-5.10.234-lvc45 от 06 марта 2025 года (Enzo Matsumiya <ematsumiya@suse.de>, бэкпортирован Anastasia Belova <abelova@astralinux.ru>)
- CVE-2024-56608 "drm/amd/display: Fix out-of-bounds access in 'dcn21_link_encoder_create'" (Уровень опасности 7.8) - была устранена в linux-5.10.235-lvc47 от 28 марта 2025 года (Srinivasan Shanmugam <srinivasan.shanmugam@amd.com>, бэкпортирован Mikhail Ilin <m.ilin@mt-integration.ru>)
- BDU:2025-00065 (CVE-2024-50280) "dm cache: fix flushing uninitialized delayed_work on cache_ctr error" (Уровень опасности

Примеры результатов анализа

[АНОНС] Релиз ядра linux-5.10.236-lvc50	Alexey Khoroshilov	25.04.2025, 09:37
[АНОНС] Релиз ядра linux-6.1.134-lvc22	Alexey Khoroshilov	25.04.2025, 11:06
[АНОНС] Кандидат на релиз ядра linux-5.10.236-lvc51-rc1	Alexey Khoroshilov	28.04.2025, 14:36
[АНОНС] Кандидат на релиз ядра linux-6.1.135-lvc23-rc1	Alexey Khoroshilov	29.04.2025, 13:36
[АНОНС] Релиз ядра linux-5.10.236-lvc51	Alexey Khoroshilov	03.05.2025, 17:11
[АНОНС] Релиз ядра linux-6.1.135-lvc23	Alexey Khoroshilov	03.05.2025, 17:58
[АНОНС] Кандидат на релиз ядра linux-6.1.136-lvc24-rc1	Alexey Khoroshilov	04.05.2025, 20:38
[АНОНС] Кандидат на релиз ядра linux-5.10.237-lvc52-rc1	Alexey Khoroshilov	05.05.2025, 09:58
[АНОНС] Кандидат на релиз ядра linux-5.10.237-lvc52-rc2	Alexey Khoroshilov	07.05.2025, 09:39
[АНОНС] Кандидат на релиз ядра linux-6.1.137-lvc24-rc2	Alexey Khoroshilov	07.05.2025, 11:18
[АНОНС] Релиз ядра linux-5.10.237-lvc52	Alexey Khoroshilov	12.05.2025, 09:55
[АНОНС] Релиз ядра linux-6.1.137-lvc24	Alexey Khoroshilov	12.05.2025, 09:57
[АНОНС] Кандидат на релиз ядра linux-5.10.237-lvc53-rc1	Alexey Khoroshilov	19.05.2025, 11:12
[АНОНС] Кандидат на релиз ядра linux-6.1.139-lvc25-rc1	Alexey Khoroshilov	19.05.2025, 14:45
[АНОНС] Релиз ядра linux-5.10.237-lvc53	Alexey Khoroshilov	22.05.2025, 13:26
[АНОНС] Кандидат на релиз ядра linux-6.1.139-lvc25-rc2	Alexey Khoroshilov	22.05.2025, 14:27
[АНОНС] Релиз ядра linux-6.1.139-lvc25	Alexey Khoroshilov	29.05.2025, 20:12
[АНОНС] Кандидат на релиз ядра linux-5.10.237-lvc54-rc1	Alexey Khoroshilov	04.06.2025, 12:07
[АНОНС] Кандидат на релиз ядра linux-6.1.140-lvc26-rc1	Alexey Khoroshilov	04.06.2025, 15:00
[АНОНС] Релиз ядра linux-5.10.237-lvc54	Alexey Khoroshilov	07.06.2025, 16:24
[АНОНС] Релиз ядра linux-6.1.140-lvc26	Alexey Khoroshilov	07.06.2025, 20:33
[АНОНС] Кандидат на релиз ядра linux-6.1.141-lvc27-rc1	Alexey Khoroshilov	13.06.2025, 00:43
[АНОНС] Кандидат на релиз ядра linux-5.10.238-lvc55-rc1	Alexey Khoroshilov	13.06.2025, 14:08
[АНОНС] Кандидат на релиз ядра linux-6.1.141-lvc27-rc2	Alexey Khoroshilov	17.06.2025, 21:30
[АНОНС] Кандидат на релиз ядра linux-5.10.238-lvc55-rc2	Alexey Khoroshilov	17.06.2025, 21:33

Примеры результатов анализа

Subject **[АНОНС] Кандидат на релиз ядра linux-6.1.141-lvc27-rc2** 17.06.2025, 21:30

To lvc-expert-group@linuxtesting.org <lvc-expert-group@linuxtesting.org>

Добрый вечер!

В связи с тем, что фаззинг-тестирование кандидата на релиз ядра linux-6.1.141-lvc27-rc1 выявило ошибку "WARNING: refcount bug in tipc_crypto_xmit", которая приводит к записи в уже освобождённую память или падению при срабатывании предупреждения, подготовлен кандидат на релиз ядра linux-6.1.139-lvc25-rc2 [1]. Для исправления проблемы добавлен патч, уже присутствующий в основной ветки ядра "net: tipc: fix refcount warning in tipc_aead_encrypt" (Charalampos Mitrodimas <charmitro@posteo.net>, бэкпортирован Fedor Pchelkin <pchelkin@ispras.ru>).

Полный список изменений кандидата на релиз ядра linux-6.1.141-lvc27-rc2 относительно linux-6.1.140-lvc26 включает в себя:

Примеры результатов анализа

From Me <khoroshilov@ispras.ru>

Reply | Forward | Archive | Junk | Delete | More

Subject **[АНОНС] Кандидат на релиз ядра linux-5.10.230-lvc39-rc2**

10.12.2024, 09:52

To lvc-expert-group@linuxtesting.org <lvc-expert-group@linuxtesting.org>

Доброе утро!

В связи с тем, что тестирование кандидата на релиз ядра linux-5.10.230-lvc39-rc1 выявило ошибку, внесённую патчем "scsi: core: Fix scsi_mode_sense() buffer length handling" (Damien Le Moal <damien.lemoal@wdc.com>, бэкпортирован Vasiliy Kovalev <kovalev@altlinux.org>), устраняющий уязвимость BDU:2024-09142 (CVE-2021-47182) (уровень опасности Высокий, 8,8), подготовлен кандидат на релиз ядра linux-5.10.230-lvc39-rc2 [1].

Проблема может приводить к некорректному выполнению SCSI дисками SCSI команд типа MODE SENSE в 10-байтовом варианте.
Детали см. в обсуждении к билету:
https://gitlab.linuxtesting.ru/lvc/kernel-bdu/-/issues/2

Проблема выявлена в ходе функционального тестирования при помощи тестового набора blktests.
Для её исправления выполнено бэкпортирование дополнительного патча:
- "scsi: sd: Fix sd_do_mode_sense() buffer length handling"

Примеры результатов анализа

From Me <khoroshilov@ispras.ru>

Reply | Forward | Archive | Junk | Delete | More

Subject **[АНОНС] Кандидат на релиз ядра linux-6.1.119-lvc10-rc2**

01.12.2024, 18:16

To lvc-expert-group@linuxtesting.org <lvc-expert-group@linuxtesting.org>

Добрый день!

В связи с тем, что тестирование кандидата на релиз ядра linux-6.1.119-lvc10-rc1 выявило ошибку, внесённую в базовую версию 6.1.119 патчем "net/sched: taprio: extend minimum interval restriction to entire cycle too" (коммит 34d83c3e6e97867ae061d14eb52123404aab1cbc), подготовлен кандидат на релиз ядра linux-6.1.119-lvc10-rc2 [1].

Проблема может приводить к срабатыванию WARNING в ядре при действиях, выполняемых непривилегированным пользователем, что может быть критично для систем, функционирующих с выставленной настройкой panic_on_warn=1.

Проблема выявлена при помощи фаззинг-тестирования. Для её исправления в нашу ветку добавлен патч "net/sched: taprio: make q->picos_per_byte available to fill_sched_entry()" (Vladimir Oltean <vladimir.oltean@nxp.com>, бэкпортирован Fedor Pchelkin <pchelkin@ispras.ru>).

Полный список изменений кандидата на релиз ядра linux-6.1.119-lvc10-rc2

Примеры результатов анализа

From Me <khoroshilov@ispras.ru>

Reply | Forward | Archive | Junk | Delete | More

Subject **[АНОНС] Кандидат на релиз ядра linux-5.10.229-lvc37-rc2**

11.11.2024, 11:18

To lvc-expert-group@linuxtesting.org <lvc-expert-group@linuxtesting.org>

Добрый день!

В связи с выявлением проблем в бэкпортированных патчах:
- "btrfs: do not BUG_ON() when freeing tree block after error" (Filipe Manana <fdmanana@suse.com>, бэкпортирован Artem Sadovnikov <ancowi69@gmail.com>), устраняющий ошибку "BUG in btrfs_free_tree_block"(https://gitlab.linuxtesting.ru/lvc/kernel-issues/-/issues/113).
- "perf/x86/intel: Fix PEBS-via-PT reload base value for Extended PEBS" (Like Xu <like.xu.linux@gmail.com>, бэкпортирован Murad Masimov <m.masimov@maxima.ru>), устраняющий ошибку BUFFER_OVERFLOW.EX: arch/x86/events/intel/ds.c:1146.
кандидат на релиз ядра linux-5.10.228-lvc37-rc1 признан не готовым к выпуску.

Подготовлен кандидат на релиз ядра linux-5.10.229-lvc37-rc2 [1], в котором:

1. В качестве базовой версии ядра Linux используется версия 5.10.229 (вместо 5.10.228).

Примеры результатов анализа

From Me <khoroshilov@ispras.ru>

Reply | Forward | Archive | Junk | Delete | More

Subject [АНОНС] Кандидат на релиз ядра linux-5.10.229-lvc37-rc2 11.11.2024, 11:18

```
5182    * NOTE: return value 1 means we should stop walking up.
5183    */
5184   static noinline int walk_up_proc(struct btrfs_trans_handle *trans,
5185                                    struct btrfs_root *root,
5186                                    struct btrfs_path *path,
5187                                    struct walk_control *wc)
5188   {
5189       struct btrfs_fs_info *fs_info = root->fs_info;
5190       int ret;
5191       int level = wc->level;
5192       struct extent_buffer *eb = path->nodes[level];
5193       u64 parent = 0;
5194
5195       if (wc->stage == UPDATE_BACKREF) {
5196           BUG_ON(wc->shared_level < level);
5197           if (level < wc->shared_level)
5198               goto out;
5199
5288   out:
5289       wc->refs[level] = 0;
5290       wc->flags[level] = 0;
```

Undecided | Unspecified | Undecided

UNINIT.LOCAL_VAR Uninitialized data is read from local

Примеры результатов анализа

From Me <khoroshilov@ispras.ru>

Reply | Forward | Archive | Junk | Delete | More

Subject [АНОНС] Кандидат на релиз ядра linux-5.10.229-lvc37-rc2 11.11.2024, 11:18

```
5182    * NOTE: return value 1 means we should stop walking up.
5183    */
5184   static noinline int walk_up_proc(struct btrfs_trans_handle *trans,
5185                                    struct btrfs_root *root,
5186                                    struct btrfs_path *path,
5187                                    struct walk_control *wc)
5188   {
5189       struct btrfs_fs_info *fs_info = root->fs_info;
5190       int ret;
5191       int level = wc->level;
```

v6
- v6.13
- v6.12
  - v6.12.4
  - v6.12.3
  - v6.12.2
  - v6.12.1
  - v6.12
  - v6.12-rc7
  - v6.12-rc6
  - v6.12-rc5
  - v6.12-rc4

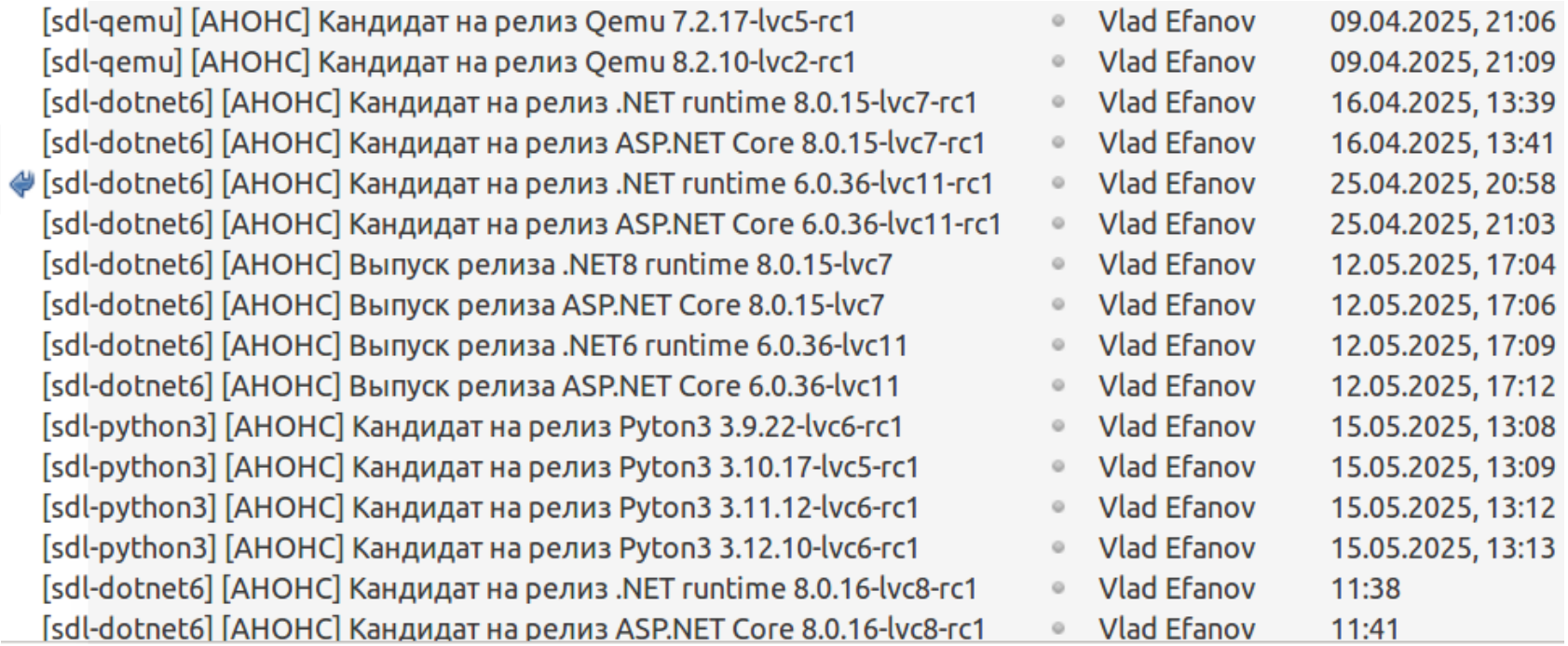
```
5798    * NOTE: return value 1 means we should stop walking up.
5799    */
5800   static noinline int walk_up_proc(struct btrfs_trans_handle *trans,
5801                                    struct btrfs_root *root,
5802                                    struct btrfs_path *path,
5803                                    struct walk_control *wc)
5804   {
5805           struct btrfs_fs_info *fs_info = root->fs_info;
5806           int ret = 0;
5807           int level = wc->level;
5808           struct extent_buffer *eb = path->nodes[level];
5809           u64 parent = 0;
5810
5811           if (wc->stage == UPDATE_BACKREF) {
```

Примеры результатов анализа

Виртуализация
- **Qemu**

Python
- **CPython**

.NET
- **.NET Runtime**
- **ASP.NET Core**



[sdl-qemu] [АНОНС] Кандидат на релиз Qemu 7.2.17-lvc5-rc1	Vlad Efanov	09.04.2025, 21:06
[sdl-qemu] [АНОНС] Кандидат на релиз Qemu 8.2.10-lvc2-rc1	Vlad Efanov	09.04.2025, 21:09
[sdl-dotnet6] [АНОНС] Кандидат на релиз .NET runtime 8.0.15-lvc7-rc1	Vlad Efanov	16.04.2025, 13:39
[sdl-dotnet6] [АНОНС] Кандидат на релиз ASP.NET Core 8.0.15-lvc7-rc1	Vlad Efanov	16.04.2025, 13:41
[sdl-dotnet6] [АНОНС] Кандидат на релиз .NET runtime 6.0.36-lvc11-rc1	Vlad Efanov	25.04.2025, 20:58
[sdl-dotnet6] [АНОНС] Кандидат на релиз ASP.NET Core 6.0.36-lvc11-rc1	Vlad Efanov	25.04.2025, 21:03
[sdl-dotnet6] [АНОНС] Выпуск релиза .NET8 runtime 8.0.15-lvc7	Vlad Efanov	12.05.2025, 17:04
[sdl-dotnet6] [АНОНС] Выпуск релиза ASP.NET Core 8.0.15-lvc7	Vlad Efanov	12.05.2025, 17:06
[sdl-dotnet6] [АНОНС] Выпуск релиза .NET6 runtime 6.0.36-lvc11	Vlad Efanov	12.05.2025, 17:09
[sdl-dotnet6] [АНОНС] Выпуск релиза ASP.NET Core 6.0.36-lvc11	Vlad Efanov	12.05.2025, 17:12
[sdl-python3] [АНОНС] Кандидат на релиз Pyton3 3.9.22-lvc6-rc1	Vlad Efanov	15.05.2025, 13:08
[sdl-python3] [АНОНС] Кандидат на релиз Pyton3 3.10.17-lvc5-rc1	Vlad Efanov	15.05.2025, 13:09
[sdl-python3] [АНОНС] Кандидат на релиз Pyton3 3.11.12-lvc6-rc1	Vlad Efanov	15.05.2025, 13:12
[sdl-python3] [АНОНС] Кандидат на релиз Pyton3 3.12.10-lvc6-rc1	Vlad Efanov	15.05.2025, 13:13
[sdl-dotnet6] [АНОНС] Кандидат на релиз .NET runtime 8.0.16-lvc8-rc1	Vlad Efanov	11:38
[sdl-dotnet6] [АНОНС] Кандидат на релиз ASP.NET Core 8.0.16-lvc8-rc1	Vlad Efanov	11:41

Участники Центра

- **АО «Аладдин Р.Д.»**
- **ООО «Айдеко»**
- ГК «Актив»
- **ООО Фирма «АНКАД»**
- ООО «А-Реал Консалтинг»
- АО «АСКОН»
- АО «НТЦ «Атлас»
- **АО «БАРС Груп»**
- **ООО «Базальт СПО»**
- **ООО «БАЗИС»**
- **ООО «БЕЛЛСОФТ»**
- **ООО «БИЗон»**
- ООО «Веблок»
- **ООО «ВК Цифровые технологии»**
- ООО «Газинформсервис»
- ООО «Гарда Технологии»
- **АО «ИВК»**
- ООО «Е5»
- **ЗАО «Защита электронных технологий»**
- **ООО «Инферит»**
- АО «ИнфоВотч»
- **АО «ИнфоТеКС»**
- **ООО «ИТБ»**
- **АО «Лаборатория Касперского»**
- **ООО «МТ-Интеграция»**
- **ООО «Киберпротект»**
- **ООО «Клауд Солюшенс»**
- **ООО «КНС ГРУПП»**
- **ООО «Код Безопасности»**
- **ООО «Конфидент»**
- ООО «Корбит»
- ООО «Кросстех Солюшнс Групп»
- **ООО «Национальный каталог»**
- АО «НИКИРЭТ»
- ООО «НПЦ «КСБ»
- **АО «МЦСТ»**
- **АО «НИЦ ЦТ»**
- **ООО «ОРИОН»**
- **ООО «Открытая мобильная платформа»**
- **АО «НППКТ»**
- **ООО «ПиЭлСи Технолоджи»**
- **ООО «Постгрес Профессиональный»**
- **АО «РАСУ»**
- ООО «Р-Вижн»
- **ООО «РЕД СОФТ»**
- ООО «РТТ»
- **ООО «РусБИТех-Астра»**
- **ФГУП «РФЯЦ-ВНИИЭФ»**
- ООО «САФИБ»
- **АО МВП «Свемел»**
- **ООО «Системные решения»**
- **ООО «СОЛАР Секьюрити»**
- ООО «С-Терра СиЭсПи»
- ООО «Стройформ»
- **ООО «НТЦ ИТ РОСА»**
- **ООО «ТехАргос»**
- ООО «ТСС»
- ООО «Фактор-ТС»
- **АО «Флант»**
- ООО НТЦ «Фобос-НТ»
- **АО «ФИНТЕХ»**
- ООО «Электра»
- ООО «ЭнДжиАр Софтлаб»
- **АО «НПО «Эшелон»**
- **ООО «Юзергейт»**
- **ООО «ЯНДЕКС.ОБЛАКО»**

- ФГБОУ ВО «Вологодский государственный университет»
- ФГБОУ ВО «Воронежский государственный университет»
- ФГБОУ ВО «МЭИ»
- ФГБОУ ВО «МГТУ им. Н.Э. Баумана»
- ФГБОУ ВО «МИРЭА – Российский технологический университет

Совместная работа — статический анализ

06 июня 2025 – m10

	Назначено	В работе	Подтверждено							Won't Fixed				False Positive			
			На оценке	В работе	Сообщено	Исправлено	в 5.10	в 6.1	Всего	Без вериф.	Обсуждается	Подтверждено	Всего	Без вериф.	Обсуждается	Подтверждено	Всего
01-axiom	1020	-	-	66	7	49	4	-	126	354	-	285	639	92	-	163	255
02-basealt	740	-	-	51	4	18	3	-	76	241	-	390	631	8	-	25	33
03-astralinux	780	-	-	24	15	40	18	10	98	130	-	359	489	43	-	150	193
04-rosa	940	-	-	33	12	30	-	3	78	302	-	327	629	109	1	123	233
05-ivk	740	1	3	66	8	27	4	2	108	127	2	314	443	58	-	130	188
06-redsoft	980	28	-	82	3	25	3	2	115	308	22	284	614	63	11	149	223
07-yandex	900	-	-	51	9	19	10	6	90	225	-	328	553	75	-	182	257
08-aladdin	940	-	-	98	1	47	5	2	153	352	-	280	632	26	-	129	155
09-mcst	980	-	-	49	21	79	6	3	155	307	1	415	723	15	-	87	102
10-omp	780	-	-	20	48	81	3	-	152	157	-	292	449	55	-	124	179
12-securitycode	860	120	-	43	10	25	2	-	80	294	3	202	499	38	4	119	161
13-infotecs	740	-	-	37	-	21	22	10	81	219	-	226	445	43	-	171	214
14-swemel	900	-	-	26	5	47	5	11	90	358	-	378	736	5	-	69	74
15-fintech	780	-	-	7	-	44	61	34	119	261	-	301	562	13	-	86	99
16-factor-ts	195	1	-	7	10	3	3	-	23	23	-	89	112	9	-	50	59
17-confident	860	-	5	47	1	15	2	-	70	241	3	216	460	150	1	179	330
18-rasu	940	1	-	24	-	17	5	2	47	294	1	421	716	40	1	135	176
19-itb	920	101	-	128	-	25	-	-	153	148	-	293	441	79	-	146	225
20-ideco	760	120	16	66	-	15	1	-	98	254	21	209	484	13	2	43	58
21-nppct	980	-	-	22	4	16	8	10	52	344	-	458	802	23	-	103	126
22-usergate	980	3	-	59	2	22	2	2	85	329	2	549	880	1	-	11	12
23-vniief	580	13	3	1	-	1	-	-	5	161	9	307	477	27	1	57	85
24-msvsphere	740	-	-	11	98	51	1	1	161	183	-	188	371	83	-	125	208
25-ancud	860	4	29	47	5	40	4	-	125	169	9	267	445	103	7	176	286
26-t-argos	562	-	-	40	20	51	2	9	120	108	1	221	330	22	-	90	112
27-plc	960	99	-	61	-	24	-	-	85	187	8	405	600	51	3	122	176
28-yadro	640	20	-	43	-	24	-	-	67	170	-	274	444	8	-	101	109
29-maxima	740	-	-	9	3	82	4	12	106	207	-	379	586	3	-	45	48
30-corebit	110	54	-	12	-	-	-	-	12	18	-	20	38	4	-	2	6
31-crpt	540	-	-	41	-	54	-	-	95	146	9	190	345	26	2	72	100
32-cyberprotect	280	22	-	34	2	26	-	1	63	44	5	111	160	24	2	9	35
33-kaspersky	180	33	-	3	2	4	-	-	9	40	2	53	95	10	-	33	43
34-basis	120	80	1	5	-	-	-	-	6	5	-	26	31	-	-	3	3
35-acloud	100	69	-	3	-	-	-	-	3	-	1	24	25	-	-	3	3
36-rusteletech	20	20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
37-spacevm	20	1	8	-	-	-	-	-	8	-	-	-	-	7	-	4	11
Всего:	24167	790	65	1316	290	1022		120	2914	6706	99	9081	15886	1326	35	3216	4577

- 99.9% предупреждений уровня Критичный, 88% верифицировано
- 84.7% предупреждений уровня Важный, 56% верифицировано
- 65.1% предупреждений уровня Средний, 69% верифицировано

Совместная работа — фаззинг-тестирование

SDL Community v2 / Python3 / **Python3-org**

				репозиторий	
		fuzz_unicodedata_normalize	Терешин Святослав, ООО НТЦ «Фобос-НТ»	Добавлена в репозиторий	
		fuzz_io_textio_read	Терешин Святослав, ООО НТЦ «Фобос-НТ»	Добавлена в репозиторий	
		fuzz_datetime_fromisoformat	Терешин Святослав, ООО НТЦ «Фобос-НТ»	Добавлена в репозиторий	
		python_script	Сергеев Денис, ООО «Базальт СПО»	Добавлена в репозиторий	Отчет
		fuzz_time	Бурков Егор, ООО «Р-Вижн»	В работе	Отчет
PyYaml		fuzz_emmiter	Королев Валерий, ООО «Гарда Технологии»	Добавлена в репозиторий	
		fuzz_loader	Королев Валерий, ООО «Гарда Технологии»	Добавлена в репозиторий	
		fuzz_reader	Королев Валерий, ООО «Гарда Технологии»	Добавлена в репозиторий	
Audit-userspace			Воронин Дмитрий, АО «НППКТ»	В работе	Отчет
JSON			Польский Валерий, ООО «Р-Вижн»	В работе	Отчет
jinja2			Хахаев Ахмед, ООО «ЭнДжиАр Софтлаб»	В работе	
Requests			Королев Валерий, ООО «Гарда Технологии»	В работе	Отчет
Flask			Хахаев Ахмед, ООО «ЭнДжиАр Софтлаб»	В работе	Отчет

Заключение

- Доверенный open-source в корпоративном репозитории
  - open-source в корпоративном репозитории
    - Композиционный анализ
  - Приоритизация компонентов (ПА и ФБ)
  - Контролируемое доверие в корпоративном контуре
    - Проверенный open-source в корпоративном репозитории
  - Совместная работа с сообществом и другими пользователями

LinuxTesting .org

Спасибо!

Алексей Хорошилов
khoroshilov@ispras.ru
https://portal.linuxtesting.ru/
ИСП РАН
Институт системного программирования им. В.П. Иванникова РАН