

*Центр исследований безопасности
системного программного обеспечения:
настоящее и будущее*



Алексей Хорошилов
khoroshilov@ispras.ru



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

Настоящее

- Ядро Linux
 - **поддерживаются ветки 5.10 и 6.1**

Поддерживаются ветки 5.10 и 6.1

☆	[АНОНС] Релиз ядра linux-6.1.118-lvc9	• Alexey Khoroshilov	24.11.2024, 16:30
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.119-lvc10-rc1	• Alexey Khoroshilov	27.11.2024, 12:14
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.119-lvc10-rc2	• Alexey Khoroshilov	01.12.2024, 18:16
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.230-lvc39-rc1	• Alexey Khoroshilov	03.12.2024, 09:22
☆	[АНОНС] Релиз ядра linux-6.1.119-lvc10	• Alexey Khoroshilov	09.12.2024, 20:26
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.230-lvc39-rc2	• Alexey Khoroshilov	10.12.2024, 09:52
☆	[АНОНС] Релиз ядра linux-5.10.230-lvc39	• Alexey Khoroshilov	13.12.2024, 21:47
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.121-lvc11-rc1	• Alexey Khoroshilov	24.12.2024, 13:34
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.232-lvc40-rc1	• Alexey Khoroshilov	25.12.2024, 16:54
☆	[АНОНС] Релиз ядра linux-6.1.121-lvc11	• Alexey Khoroshilov	30.12.2024, 23:36
☆	[АНОНС] Релиз ядра linux-5.10.232-lvc40	• Alexey Khoroshilov	31.12.2024, 00:23
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.123-lvc12-rc1	• Alexey Khoroshilov	06.01.2025, 10:40
☆	[АНОНС] Релиз ядра linux-6.1.123-lvc12	• Alexey Khoroshilov	10.01.2025, 21:13
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.233-lvc41-rc1	• Alexey Khoroshilov	13.01.2025, 09:32
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.124-lvc13-rc1	• Alexey Khoroshilov	13.01.2025, 09:44
☆	[АНОНС] Релиз ядра linux-6.1.124-lvc13	• Alexey Khoroshilov	20.01.2025, 09:30
☆	[АНОНС] Релиз ядра linux-5.10.233-lvc41	• Alexey Khoroshilov	20.01.2025, 11:23
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.127-lvc14-rc1	• Alexey Khoroshilov	25.01.2025, 17:45
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.233-lvc42-rc1	• Alexey Khoroshilov	25.01.2025, 18:15
☆	[АНОНС] Релиз ядра linux-6.1.127-lvc14	• Alexey Khoroshilov	30.01.2025, 19:14
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.233-lvc42-rc2	• Alexey Khoroshilov	01.02.2025, 11:26
☆	[АНОНС] Релиз ядра linux-5.10.233-lvc42	• Alexey Khoroshilov	04.02.2025, 23:14
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.234-lvc43-rc1	• Alexey Khoroshilov	09.02.2025, 16:03
★	[АНОНС] Кандидат на релиз ядра linux-6.1.128-lvc15-rc1	• Alexey Khoroshilov	09.02.2025, 16:38

From Me <khoroshilov@ispras.ru> ★

↩ Reply

➡ Forward

📁 Archive

🔥 Junk

🗑 Delete

Me

Subject [АНОНС] Кандидат на релиз ядра linux-6.1.128-lvc15-rc1

09.02.2025,

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

Добрый день!

Подготовлен кандидат на релиз ядра linux-6.1.128-lvc15-rc1 [1], в котором:

Поддерживаются ветки 5.10 и 6.1

20/01/2025

РЕЛИЗ ЯДРА LINUX-5.10.233-LVC41

Опубликован релиз ядра [linux-5.10.233-lvc41](#). В качестве базовой версии ядра Linux используется версия 5.10.233 (вместо 5.10.232), в которую вошли следующие доработки:

[Читать дальше](#)

1. Исправления следующих уязвимостей:

- BDU:2024-06751 (CVE-2024-44985) "ipv6: prevent possible UAF in ip6_xmit()" (Уровень опасности 7.8)
- BDU:2024-06753 (CVE-2024-44986) "ipv6: fix possible UAF in ip6_finish_output2()" (Уровень опасности 7.8)
- CVE-2024-50121 "nfsd: cancel nfsd_shrinker_work using sync mode in nfs4_state_shutdown_net" (Уровень опасности 7.8)
- CVE-2024-56759 "btrfs: fix use-after-free when COWing tree block and tracing is enabled" (Уровень опасности 7.8)
- CVE-2024-56766 "mtd: rawnand: fix double free in atmel_pmecc_create_user()" (Уровень опасности 7.8)
- CVE-2024-53099 "bpf: Check validity of link->type in bpf_link_show_fdinfo()" (Уровень опасности 7.1)
- CVE-2024-56769 "media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg" (Уровень опасности 5.5),
 - патч, разработанный Nikita Zhandarovich <n.zhandarovich@fintech.ru> и устраняющий ошибку "KMSAN: uninit-value in dib3000mb_attach (2)"(<https://gitlab.linuxtesting.ru/lvc/kernel-issues/-/issues/178>)
- CVE-2024-56694 "bpf: fix recursive lock when verdict program return SK_PASS" (Уровень опасности 5.5)
- CVE-2024-56767 "dmaengine: at_xdmac: avoid null_ptr_deref in at_xdmac_prep_dma_memset" (Уровень опасности 5.5)
- CVE-2024-56763 "tracing: Prevent bad count for tracing_cpumask_write" (Уровень опасности 5.5)



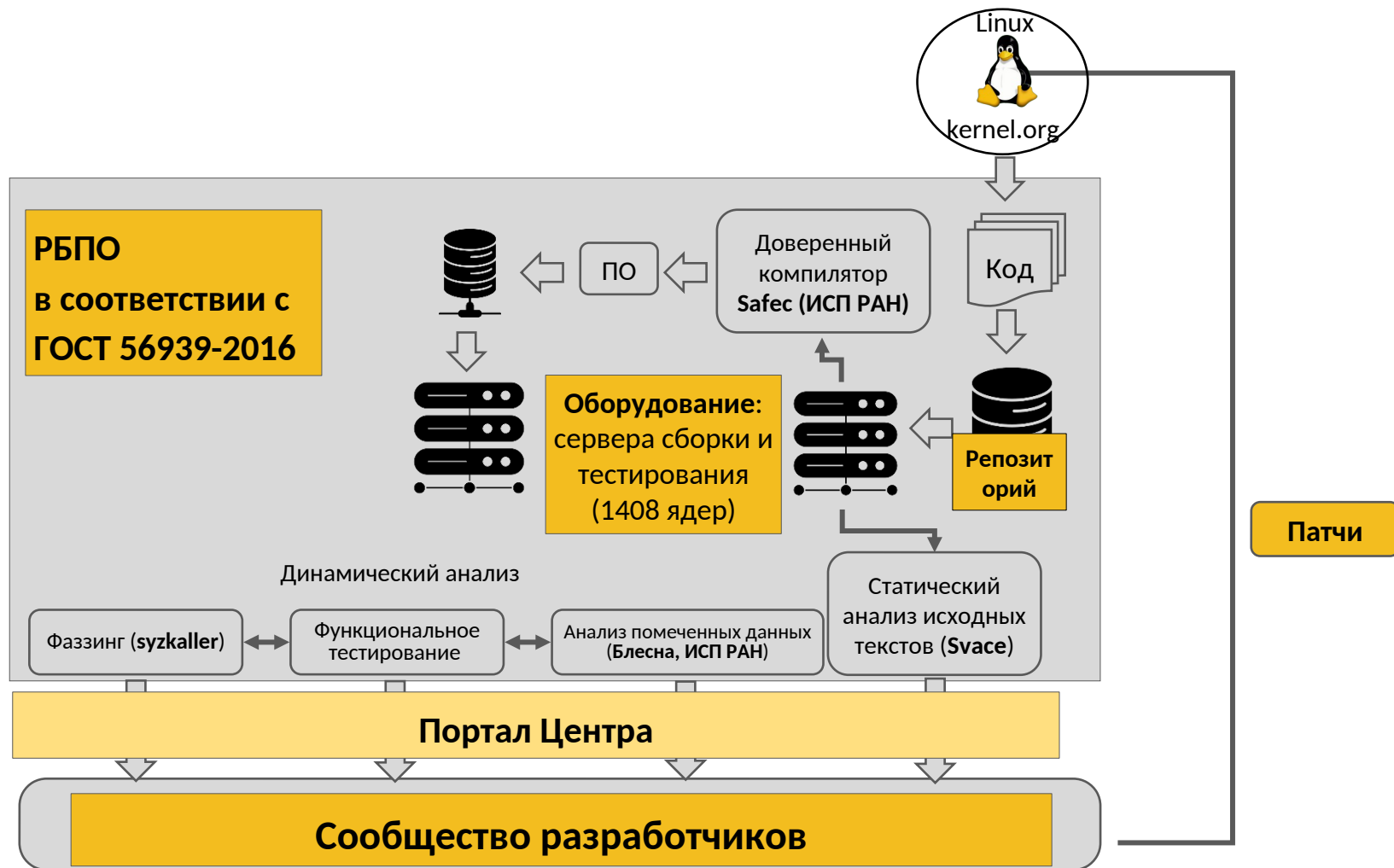
Поддерживаются ветки 5.10 и 6.1

2. Добавлен патч "smb: client: fix use-after-free bug in cifs_debug_data_proc_show()" (Paulo Alcantara <pc@manguebit.com>, бэкпортирован Dmitriy Privalov <d.privalov@omp.ru>), устраняющий уязвимость BDU:2024-04576 (CVE-2023-52752) (Уровень опасности 7.8).
3. Добавлен патч "nvme: avoid double free special payload" (Chunguang Xu <chunguang.xu@shopee.com>, бэкпортирован Dmitriy Privalov <d.privalov@omp.ru>), устраняющий уязвимость BDU:2024-08315 (CVE-2024-41073) (Уровень опасности 7.8).
4. Добавлен патч "ext4: fix timer use-after-free on failed mount" (Xiayi Shen <shenxiayi26@gmail.com>, бэкпортирован Dmitriy Privalov <d.privalov@omp.ru>), устраняющий уязвимость BDU:2024-09005 (CVE-2024-49960) (Уровень опасности 7.8).
5. Добавлена серия патчей
 - "x86/kasan: Map shadow for percpu pages on demand" (Andrey Ryabinin <ryabinin.a.a@gmail.com>, бэкпортирован Vasiliy Kovalev <kovalev@altlinux.org>)
 - "x86/mm: Recompute physical address for every page of per-CPU CEA mapping" (Sean Christopherson <seanjc@google.com>, бэкпортирован Vasiliy Kovalev <kovalev@altlinux.org>)
 - "x86/mm: Populate KASAN shadow for entire per-CPU range of CPU entry area" (Sean Christopherson <seanjc@google.com>, бэкпортирован Vasiliy Kovalev <kovalev@altlinux.org>)
 - "x86/mm: Randomize per-cpu entry area" (Peter Zijlstra <peterz@infradead.org>, бэкпортирован Vasiliy Kovalev <kovalev@altlinux.org>)
 - "x86/mm: Do not shuffle CPU entry areas without KASLR" (Michal Koutny <mkoutny@suse.com>, бэкпортирован Vasiliy Kovalev <kovalev@altlinux.org>) устраняющая уязвимости BDU:2023-00625 (Уровень опасности 5.5) и BDU:2023-03962 (Уровень опасности 7.8).
6. Добавлен патч "media: v4l2-ctrls-core.c: check min/max for menu, controls" (Hans Verkuil <hverkuil-cisco@xs4all.nl>, бэкпортирован Roman Smirnov <r.smirnov@omp.ru>), устраняющий ошибки "UBSAN: shift-out-of-bounds in drivers/media/v4l2-core/v4l2-ctrls.c" и "NO_CAST.INTEGER_OVERFLOW: drivers/media/v4l2-core/v4l2-

Настоящее

- Ядро Linux
 - поддерживаются ветки 5.10 и 6.1
 - **настроены процессы автоматического анализа**
 - **статический анализ**
 - **функциональное тестирование**
 - **фаззинг-тестирование**

Настроены процессы автоматического анализа



2021

Началось сопровождение ветки ядра, основанной на стабильной версии 5.10

2023

Сопровождение ведется в режиме реального времени на постоянной основе

2023-2024

Добавление работ с дополнительной версией ядра: 6.1 (стабильная ветка)

Настроены процессы автоматического анализа

☆	[АНОНС] Релиз ядра linux-6.1.118-lvc9	• Alexey Khoroshilov	24.11.2024, 16:30
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.119-lvc10-rc1	• Alexey Khoroshilov	27.11.2024, 12:14
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.119-lvc10-rc2	• Alexey Khoroshilov	01.12.2024, 18:16
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.230-lvc39-rc1	• Alexey Khoroshilov	03.12.2024, 09:22
☆	[АНОНС] Релиз ядра linux-6.1.119-lvc10	• Alexey Khoroshilov	09.12.2024, 20:26
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.230-lvc39-rc2	• Alexey Khoroshilov	10.12.2024, 09:52
☆	[АНОНС] Релиз ядра linux-5.10.230-lvc39	• Alexey Khoroshilov	13.12.2024, 21:47
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.121-lvc11-rc1	• Alexey Khoroshilov	24.12.2024, 13:34
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.232-lvc40-rc1	• Alexey Khoroshilov	25.12.2024, 16:54
☆	[АНОНС] Релиз ядра linux-6.1.121-lvc11	• Alexey Khoroshilov	30.12.2024, 23:36
☆	[АНОНС] Релиз ядра linux-5.10.232-lvc40	• Alexey Khoroshilov	31.12.2024, 00:23
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.123-lvc12-rc1	• Alexey Khoroshilov	06.01.2025, 10:40
☆	[АНОНС] Релиз ядра linux-6.1.123-lvc12	• Alexey Khoroshilov	10.01.2025, 21:13
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.233-lvc41-rc1	• Alexey Khoroshilov	13.01.2025, 09:32
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.124-lvc13-rc1	• Alexey Khoroshilov	13.01.2025, 09:44
☆	[АНОНС] Релиз ядра linux-6.1.124-lvc13	• Alexey Khoroshilov	20.01.2025, 09:30
☆	[АНОНС] Релиз ядра linux-5.10.233-lvc41	• Alexey Khoroshilov	20.01.2025, 11:23
☆	[АНОНС] Кандидат на релиз ядра linux-6.1.127-lvc14-rc1	• Alexey Khoroshilov	25.01.2025, 17:45
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.233-lvc42-rc1	• Alexey Khoroshilov	25.01.2025, 18:15
☆	[АНОНС] Релиз ядра linux-6.1.127-lvc14	• Alexey Khoroshilov	30.01.2025, 19:14
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.233-lvc42-rc2	• Alexey Khoroshilov	01.02.2025, 11:26
☆	[АНОНС] Релиз ядра linux-5.10.233-lvc42	• Alexey Khoroshilov	04.02.2025, 23:14
☆	[АНОНС] Кандидат на релиз ядра linux-5.10.234-lvc43-rc1	• Alexey Khoroshilov	09.02.2025, 16:03
★	[АНОНС] Кандидат на релиз ядра linux-6.1.128-lvc15-rc1	• Alexey Khoroshilov	09.02.2025, 16:38

From Me <khoroshilov@ispras.ru> ★

↩ Reply

→ Forward

📁 Archive

🔥 Junk

🗑 Delete

Me

Subject [АНОНС] Кандидат на релиз ядра linux-6.1.128-lvc15-rc1

09.02.2025,

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

Добрый день!

Подготовлен кандидат на релиз ядра linux-6.1.128-lvc15-rc1 [1], в котором:

Настроены процессы автоматического 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"

Полный список изменений кандидата на релиз ядра linux-5.10.230-lvc39-rc2 относительно linux-5.10.230-lvc38 включает в себя:

1. Добавлена серия патчей:

- "scsi: core: Fix scsi_mode_sense() buffer length handling" (Damien Le Moal <damien.lemoal@wdc.com>, бэкпортирован Vasiliy Kovalev <kovalev@altlinux.org>)

- "scsi: core: Fix scsi_mode_select() buffer length handling" (Damien Le Moal <damien.lemoal@wdc.com>, бэкпортирован Vasiliy Kovalev

Настроены процессы автоматического 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 относительно linux-6.1.119-lvc9 включает в себя:

1. В качестве базовой версии ядра Linux используется версия 6.1.119 (вместо 6.1.118), что включает в себя исправления следующих уязвимостей:
 - CVE-2024-44949 "parisc: fix a possible DMA corruption"
 - CVE-2024-36478 "null_blk: fix null-ptr-dereference while configuring 'power' and 'submit_queues'"
 - CVE-2022-45888 "char: xillybus: Prevent use-after-free due to race condition"

Настроены процессы автоматического 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).
2. Добавлен патч "wifi: ath10k: Check return value of ath10k_get_arvif() in ath10k_wmi_event_tlds_peer()" (Peter Kosyh <pkosyh@yandex.ru>, бэкпортирован Dmitry Kandybka <d.kandybka@gmail.com>), устраняющий ошибку Deref_of_Null.Ret: drivers/net/wireless/ath/ath10k/wmi-tlv.c:589.
3. Добавлен патч "drm/amd/display: Fix possible overflow in integer multiplication" (Alex Hung <alex.hung@amd.com>, бэкпортирован v.shevtsov@maxima.ru), устраняющий ошибку NO_CAST.INTEGER_OVERFLOW: drivers/gpu/drm/amd/display/dc/dml/calcs/dce_calcs.c:1858.

Настроены процессы автоматического 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 ninline 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      }
5200      btrfs_abort_transaction(trans, ret);
5201
5202  out:
5203      wc->refs[level] = 0;
5204      wc->flags[level] = 0;
```



Undecided

Unspecified

Undecided

UNINIT.LOCAL_VAR Uninitialized data is read from local variable 'ret' at extent-tree.c:5291.

```
5291  return ret;
```

```
5292
```

multiplication" (Alex Hung <alex.hung@amd.com>, бэкпортирован v.shevtsov@maxima.ru), устраняющий ошибку NO_CAST.INTEGER_OVERFLOW: drivers/gpu/drm/amd/display/dc/dml/calcs/dce_calcs.c:1858.

Настроены процессы автоматического 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 ninline 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
 - ▶ v6.12-rc3
 - ▶ v6.12-rc2
 - ▶ v6.12-rc1
- ▶ v6.11
- ▶ v6.10
- ▶ v6.9
- ▶ v6.8
- ▶ v6.7
- ▶ v6.6

```
5798  * NOTE: return value 1 means we should stop walking up.
5799  */
5800  static ninline 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) {
5812          ASSERT(wc->shared_level >= level);
5813          if (level < wc->shared_level)
5814              goto out;
5815
5816          ret = find_next_key(path, level + 1, &wc->update_progress);
5817          if (ret > 0)
5818              wc->update_ref = 0;
5819
5820          wc->stage = DROP_REFERENCE;
5821          wc->shared_level = -1;
5822          path->slots[level] = 0;
```

Настроены процессы автоматического анализа

From Me <khoroshilov@ispras.ru>★

↩ Reply

→ Forward

📁 Archive

🔥 Junk

🗑 Delete

More ▾

Subject [АНОНС] Кандидат на релиз ядра linux-6.1.113-lvc7-rc2

25.10.2024, 01:52

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

Добрый вечер!

В связи с тем, что тестирование кандидата на релиз ядра linux-6.1.113-lvc7-rc1 выявило ошибку, внесённую в базовую версию 6.1.113 некорректным бэкпортированием патча "wifi: mac80211: fix RCU list iterations" (коммит ac35180032fbc5d80b29af00ba4881815ceefcb6), подготовлен кандидат на релиз ядра linux-6.1.113-lvc7-rc2 [1].

Виновный патч "wifi: mac80211: fix RCU list iterations" полагается на изменения в синхронизации wiphy, принятые в основную ветку ядра в рамках серии патчей "wifi: cfg80211/mac80211: locking cleanups"[2], которые не были бэкпортированы, что приводит к гонкам по данным.

Проблемы выявлена при помощи фаззинг-тестирования. Для её исправления в нашу ветку добавлен патч, отменяющий изменения "wifi: mac80211: fix RCU list iterations".

Полный список изменений кандидата на релиз ядра linux-6.1.113-lvc7-rc2 относительно linux-6.1.112-lvc6 включает в себя:

1. В качестве базовой версии ядра Linux используется версия 6.1.113 (вместо 6.1.112).
2. Добавлен патч "clk: mvebu: Prevent division by zero in clk_double_div_recalc_rate()" (Alexandra Diupina <adiupina@astralinux.ru>), устраняющий ошибку DIVISION_BY_ZERO: drivers/clk/mvebu/armada-37xx-periph.c:347.
3. Добавлен патч "drm/amd/display: Add null pointer guards where needed" (Josip Pavic <josip.pavic@amd.com>, бэкпортирован Igor Artemiev <Igor.A.Artemiev@mcst.ru>), устраняющий ошибку Deref_of_null.ret.stat:

Настоящее

- Ядро Linux
 - поддерживаются ветки 5.10 и 6.1
 - настроены процессы автоматического анализа
 - статический анализ
 - функциональное тестирование
 - фаззинг-тестирование
 - **организован систематический процесс экспертного анализа результатов**
 - **разметка предупреждений статического анализа**
 - **разбор падений выявляемых фаззингом**
 - **исправление выявляемых недостатков**

Количество предупреждений на всём ядре

Критичные	1758
Важные	11224
Средние	9595
Низкие	15588
Всего	38165

m09 = SVACE 3.4.240516

GROUP_RESULTS_OF_STAT_CHECKERS false

GROUP_RESULTS_OF_BUFFER_OVERFLOW.PROC false

GROUP_RESULTS_OF_UNCHECKED_FUNC_RES.STAT false

GROUP_RESULTS_OF_DEREF_OF_NULL.RET.STAT false

GROUP_RESULTS_OF_NO_LOCK.STAT.EX false

GROUP_RESULTS_OF_NO_LOCK.GUARD false

Двухнедельные итерации

📁 01-Sprint_2022-05-13	Добавлено распределение задач на итерации 1-26	5 months ago
📁 02-Sprint_2022-05-27	Добавлено распределение задач на итерации 1-26	5 months ago
📁 55-Sprint_2024-07-19	Добавлено распределение задач на 55-ю итерацию	6 months ago
📁 56-Sprint_2024-08-02	Добавлено распределение задач на 56-ю итерацию	6 months ago
📁 57-Sprint_2024-08-16	Добавлено распределение задач на 57-ю итерацию	5 months ago
📁 58-Sprint_2024-08-30	Добавлено распределение задач на 58-ю итерацию	5 months ago
📁 59-Sprint_2024-09-13	Добавлено распределение задач на 59-ю итерацию	4 months ago
📁 60-Sprint_2024-09-27	Добавлено распределение задач на 60-ю итерацию	4 months ago
📁 61-Sprint_2024-10-11	Добавлено распределение задач на 61-ю итерацию	3 months ago
📁 62-Sprint_2024-10-25	Добавлено распределение задач на 62-ю итерацию	3 months ago
📁 63-Sprint_2024-11-08	Добавлено распределение задач на 63-ю итерацию	2 months ago
📁 64-Sprint_2024-11-22	Добавлено распределение задач на 64-ю итерацию	2 months ago
📁 65-Sprint_2024-12-06	Добавлено распределение задач на 65-ю итерацию	1 month ago
📁 66-Sprint_2024-12-20	Добавлено распределение задач на 66-ю итерацию	1 month ago
📁 67-Sprint_2025-01-17	Добавлено распределение задач на 67-ю итерацию	3 weeks ago
📁 68-Sprint_2025-01-31	Добавлено распределение задач на 68-ю итерацию	4 days ago

Статистика по разметке предупреждений

31 января 2025 - m09

	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-bellsoft	970	29	-	53	6	45	4	-	108	315	1	280	596	78	1	158	237
02-basealt	740	32	-	62	-	13	3	-	78	235	1	361	597	8	-	25	33
03-astralinux	780	16	-	28	17	39	17	9	102	251	-	216	467	73	-	122	195
04-rosa	940	51	-	38	10	15	-	3	66	307	13	270	590	111	4	118	233
05-ivk	740	20	2	58	4	13	2	-	79	253	14	187	454	70	-	117	187
06-redsoft	970	88	-	75	3	24	3	2	107	311	7	239	557	69	9	140	218
07-yandex	890	5	-	57	8	15	8	4	89	267	-	271	538	82	1	175	258
08-aladdin	890	2	-	96	1	46	5	2	150	329	4	254	587	23	1	127	151
09-mcst	970	-	-	48	19	72	6	3	145	355	5	364	724	17	-	84	101
10-omp	780	10	-	31	40	76	3	-	150	200	1	239	440	59	-	121	180
12-securitycode	850	110	-	43	10	25	2	-	80	297	3	199	499	43	-	118	161
13-infotecs	740	9	-	33	1	20	22	9	76	240	-	196	436	58	-	161	219
14-swemel	890	2	-	21	5	41	4	9	77	392	5	340	737	7	-	67	74
15-fintech	770	-	-	1	12	43	49	21	111	285	-	275	560	14	-	85	99
16-factor-ts	195	2	-	7	10	3	3	-	23	23	-	88	111	9	-	50	59
17-confident	850	98	4	40	1	14	2	-	61	212	2	186	400	130	1	160	291
18-rasu	930	22	-	23	-	16	5	2	45	360	3	327	690	70	2	101	173
19-itb	740	39	-	118	-	16	-	-	134	233	3	129	365	66	-	136	202
20-ideco	760	120	16	66	5	10	1	-	98	259	17	208	484	13	2	43	58
21-nppct	970	-	7	8	2	5	8	8	30	411	5	394	810	31	2	97	130
22-usergate	970	22	2	48	2	17	2	2	71	389	16	460	865	1	-	11	12
23-vniief	580	13	3	1	-	1	-	-	5	176	9	292	477	27	1	57	85
24-msvsphere	710	7	-	129	3	50	-	-	182	151	4	171	326	73	1	121	195
25-ancud	850	17	17	47	5	39	4	-	112	180	8	255	443	110	5	163	278
26-t-argos	562	-	-	42	23	49	2	9	123	111	1	215	327	24	-	88	112
27-plc	700	-	-	37	-	5	-	-	42	243	1	232	476	62	11	109	182
28-yadro	640	20	-	43	-	24	-	-	67	171	-	273	444	8	-	101	109
29-maxima	740	74	-	37	2	47	-	2	88	168	2	363	533	2	-	43	45
30-corebit	20	11	-	-	-	-	-	-	-	-	1	8	9	-	-	-	-
31-crpt	90	3	1	20	-	-	-	-	21	29	1	33	63	-	-	3	3
32-cyberprotect	60	-	-	9	-	-	-	-	9	23	-	19	42	5	-	4	9
Всего:	22287	822	52	1319	189	783		85	2529	7176	127	7344	14647	1343	41	2905	4289

- 99.9% предупреждений уровня Критичный, 89% верифицировано
- 85% предупреждений уровня Важный, 58% верифицировано
- 66% предупреждений уровня Средний, 70% верифицировано
- 33% предупреждений уровня Низкий, 19% верифицировано

Всего размечено более 34 тыс. предупреждений,
18 тыс. верифицировано

Участники исследований ядра

- АО «Аладдин Р.Д.»
- ООО «Айдеко»
- ООО Фирма «АНКАД»
- ООО «Базальт СПО»
- ООО «БЕЛЛСОФТ»
- АО «ИВК»
- ООО «Инферит»
- АО «ИнфоТеКС»
- ООО «ИТБ»
- ООО «МТ-Интеграция»
- ООО «КНС ГРУПП»
- ООО «Киберпротект»
- ООО «Код Безопасности»
- ООО «Конфидент»
- ООО «Корбит»
- АО «МЦСТ»
- ООО «Национальный каталог»
- ООО «Открытая мобильная платформа»
- АО «НППКТ»
- ООО «ПиЭлСи Технолоджи»
- АО «РАСУ»
- ООО «РЕД СОФТ»
- ООО «РусБИТех-Астра»
- ФГУП «РФЯЦ-ВНИИЭФ»
- АО МВП «Свемел»
- ООО «СОЛАР Секьюрити»
- АО «НТЦ ИТ РОСА»
- ООО «ТехАргос»
- АО «ФИНТЕХ»
- 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»

Open 5 Closed 94 All 99

Edit issues

New issue

Recent searches ▾

Label = ~Принято ✕

✕

Updated date ▾

⌵

- WARNING in drv_remove_interface**

#165 · created 3 months ago by Федор Пчелкин 29-maxima Незначительное Подтверждено Принято

21 updated 1 hour ago
- WARNING: refcount bug in ax25_release (3)**

#168 · created 3 months ago by Федор Пчелкин 29-maxima Значительное Подтверждено Принято

3 updated 20 hours ago
- WARNING in cxacru_cm/usb_submit_urb**

#111 · created 7 months ago by Никита Жандарович 15-fintech Исправлено Незначительное Подтверждено Принято

CLOSED 2 updated 1 day ago
- WARNING in to_nfit_bus_uuid**

#169 · created 3 months ago by Федор Пчелкин 29-maxima Значительное Подтверждено Принято

4 updated 4 days ago
- general protection fault in ir_raw_event_store_with_filter**

#82 · created 10 months ago by Федор Пчелкин 29-maxima Значительное Подтверждено Принято

8 updated 6 days ago
- kernel BUG in filemap_unaccount_folio**

#173 · created 2 months ago by Андрей Калачев 14-swemel Значительное Исправлено Подтверждено Принято

CLOSED 13 updated 6 days ago
- UBSAN: shift-out-of-bounds in drivers/media/v4l2-core/v4l2-ctrls.c**

#103 · created 7 months ago by Роман Смирнов 10-omp Исправлено Незначительное Подтверждено Принято

CLOSED 9 updated 3 weeks ago
- KMSAN: uninit-value in dib3000mb_attach (2)**

#178 · created 1 month ago by Никита Жандарович 15-fintech Исправлено Незначительное Подтверждено Принято

CLOSED 1 updated 1 month ago

Статистика по принятым исправлениям в ядро

	Февраль 2023 (105)	Август 2023 (190)	Февраль 2024 (275)	Июнь 2024 (352)	Февраль 2025 (503)
ООО «Айдеко»	-	0	0	0	1
АО «Аладдин Р.Д.»	0	3	5	10	11
ООО Фирма «АНКАД»	-	0	2	6	6
ООО «Базальт СПО»	1	4	4	4	4
ООО «БЕЛЛСОФТ»	7	10	10	13	14
АО «ИВК»	0	4	4	4	4
ООО «Инферит»	-	1	17	23	62
АО «ИнфоТекС»	3	9	14	15	16
ООО «ИТБ»	0	0	1	1	3
ООО «Код Безопасности»	0	3	3	3	3
ООО «Конфидент»	0	0	1	3	5
ООО «МТ-Интеграция»	-	-	-	-	12
АО «МЦСТ»	0	1	1	3	4
АО «НППКТ»	-	-	0	0	2
ООО «Открытая мобильная платформа»	24	27	38	49	53
АО «РАСУ»	3	4	5	6	6
ООО «РЕД СОФТ»	3	5	11	12	14
ООО «НТЦ ИТ РОСА»	0	0	0	4	8
ООО «РусБИТех-Астра»	6	8	13	14	20
АО МВП «Свемел»	1	4	7	8	10
ООО «ТехАргос»	-	-	0	12	34
ООО «Фактор-ТС»	4	5	5	5	5
АО «ФИНТЕХ»	4	20	24	28	51
ООО «Юзергейт»	-	0	0	2	2
ООО «ЯНДЕКС.ОБЛАКО»	5	10	12	12	14
Сотрудники центра	44	72	99	116	140

Настоящее

- Ядро Linux
 - поддерживаются ветки 5.10 и 6.1
 - настроены процессы автоматического анализа
 - статический анализ
 - функциональное тестирование
 - фаззинг-тестирование
 - организован систематический процесс экспертного анализа результатов
 - разметка предупреждений статического анализа
 - разбор падений выявляемых фаззингом
 - исправление выявляемых недостатков
 - **сформирован Консорциум**
 - **Программы исследований**
 - **бэкпортирование исправлений уязвимостей**
 - **расширение покрытия функциональными и фаззинг-тестами**

Консорциум

Соглашение о формировании Консорциума участников по поддержке Технологического центра исследования безопасности ядра Linux

г. Москва

«12» мая 2023 г.

Настоящее соглашение, заключаемое в порядке ст. 428 Гражданского Кодекса Российской Федерации, определяет порядок объединения усилий **федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук** (далее «ИСП РАН» или «Координатор Консорциума»), в лице директора Аветисяна Арутюна Ишхановича, действующего на основании Устава, и присоединившихся к настоящему Соглашению в целом образовательных организаций высшего образования, коммерческих, научных, инжиниринговых, производственных и иных организаций (далее «Участник») в целях организации эффективного взаимодействия в рамках Технологического центра исследования безопасности ядра Linux (далее «Технологический центр») для внедрения принципов безопасной разработки программного обеспечения и исключения дублирования усилий по исследованию безопасности ядра Linux.

Статья 1. Термины и определения

1.1. **Координатор Консорциума** – в качестве Координатора Консорциума выступает ИСП РАН, который осуществляет научное и методическое руководство при формировании и реализации Программы и конкретных планов развития Технологического центра.

1.2. **Координационный совет** – организационная структура, отвечающая за координацию между Участниками Консорциума, утверждение и контроль реализации Программы исследований Технологического центра, а также за решение ключевых вопросов, возникающих при исполнении данного Соглашения.

1.3. **Программа исследований Технологического центра** – документ, содержащий

УТВЕРЖДЕНО

Решением Координационного совета
Консорциума участников
по поддержке Технологического центра
исследования безопасности ядра Linux
от «29» ноября 2023 г. № 2

ПРОГРАММА ИССЛЕДОВАНИЙ

Технологического центра исследования безопасности ядра Linux
на период до 01 марта 2024 года

Настоящая Программа определяет план исследований безопасности ядра Linux на период до 01 марта 2024 года в рамках совместных работ, которые выполняются Технологическим центром безопасности ядра Linux (далее — Технологический центр) и организациями, присоединившимися к Соглашению о формировании Консорциума участников по поддержке Технологического центра исследования безопасности ядра Linux (далее — Участники).

Статья 1. Общие положения

1.1 Целью исследований является выявление и устранение потенциальных уязвимостей, недекларированных и потенциально опасных функциональных возможностей в версиях ядра Linux, поддерживаемых Технологическим центром.

1.2 Перечень версий ядра, поддерживаемых Технологическим центром, утверждается решением Координационного совета Консорциума. Актуальная версия перечня публикуется на Портале технологического центра по ссылке [1].

Программа исследований №1

- Статический анализ: 500 предупреждений
 - Confirmed — подготовить исправления все предупреждения с ненулевым влиянием на безопасность
 - «Won't Fix»/«False Positive» - обосновать решение, ответить на замечания кросс-верификации при наличии
- Фаззинг-тестирование
 - Развернуть у себя и наладить обмен результатами с Технологическим центром (10+ обменов)
- 3 задачи по «фаззинг-тестированию»
 - или Исправление падения
 - или Расширение покрытия
 - или 40 дополнительных предупреждений по статике

УТВЕРЖДЕНО

Решением Координационного совета

Консорциума участников

по поддержке Технологического центра
исследования безопасности ядра Linux

от «27» апреля 2024 г. № 3

ПРОГРАММА ИССЛЕДОВАНИЙ

Технологического центра исследования безопасности ядра Linux

на период до 01 октября 2024 года

Настоящая Программа определяет план исследований безопасности ядра Linux на период до 01 октября 2024 года в рамках совместных работ, которые выполняются Технологическим центром безопасности ядра Linux (далее — Технологический центр) и организациями, присоединившимися к Соглашению о формировании Консорциума участников по поддержке Технологического центра исследования безопасности ядра Linux (далее — Участники).

Статья 1. Общие положения

1.1 Целью исследований является выявление и устранение потенциальных уязвимостей, недекларированных и потенциально опасных функциональных возможностей

Программа исследований №2

- Статический анализ: 120 предупреждений
 - Confirmed — подготовить исправления все предупреждения с ненулевым влиянием на безопасность
 - «Won't Fix»/«False Positive» - обосновать решение, ответить на замечания кросс-верификации при наличии
- Фаззинг-тестирование
 - Развернуть у себя и наладить обмен результатами с Технологическим центром (15+ обменов)
- 3 задачи по «фаззинг-тестированию»
 - или Исправление падения
 - или Расширение покрытия
 - или 40 дополнительных предупреждений по статике

УТВЕРЖДЕНО

Решением Координационного совета
Консорциума участников
по поддержке Технологического центра
исследования безопасности ядра Linux
от «03» декабря 2024 г. № 5

ПРОГРАММА ИССЛЕДОВАНИЙ

Технологического центра исследования безопасности ядра Linux

на период до 01 мая 2025 года

Настоящая Программа определяет план исследований безопасности ядра Linux на период до 01 мая 2025 года в рамках совместных работ, которые выполняются Технологическим центром безопасности ядра Linux (далее — Технологический центр) и организациями, присоединившимися к Соглашению о формировании Консорциума участников по поддержке Технологического центра исследования безопасности ядра Linux (далее — Участники).

Статья 1. Общие положения

1.1 Целью исследований является выявление и устранение потенциальных уязвимостей, недекларированных и потенциально опасных функциональных возможностей

Программа исследований №3

- Статический анализ: 120 предупреждений
 - Confirmed — подготовить исправления все предупреждения с ненулевым влиянием на безопасность
 - «Won't Fix»/«False Positive» - обосновать решение, ответить на замечания кросс-верификации при наличии
- Фаззинг-тестирование
 - Развернуть у себя и наладить обмен результатами с Технологическим центром (15+ обменов)
- 3 задачи по «фаззинг-тестированию»
 - или Исправление падения
 - или Расширение покрытия
 - или 40 дополнительных предупреждений по статике (не более 1-й)
- **3 задачи по расширению покрытия функциональных тестов**
- **Бэкпортирование исправлений известных уязвимостей**
 - суммой не менее чем на 30.0 CVSS Score

Настоящее

- Системные компоненты
 - **поддерживаются lvs-ветки компонентов**

Поддерживаются lvc-ветки компонентов

Виртуализация

Qemu

Python

CPython

.NET

.NET Runtime

ASP.NET Core

[sdl-qemu] [АНОНС] Кандидат на релиз Qemu 7.2.15-lvc3-rc1	• Vlad Efanov	05.12.2024, 13:05
[sdl-dotnet6] [АНОНС] Выпуск релиза .NET8 runtime 8.0.8-lvc1	• Vlad Efanov	10.12.2024, 19:55
[sdl-dotnet6] [АНОНС] Выпуск релиза ASP.NET Core 8.0.8-lvc1	• Vlad Efanov	10.12.2024, 19:55
[sdl-dotnet6] [АНОНС] Выпуск релиза .NET8 runtime 8.0.10-lvc2	• Vlad Efanov	10.12.2024, 19:59
[sdl-dotnet6] [АНОНС] Выпуск релиза ASP.NET Core 8.0.10-lvc2	• Vlad Efanov	10.12.2024, 20:00
[sdl-dotnet6] [АНОНС] Кандидат на релиз .NET runtime 8.0.12-lvc4-...	• Vlad Efanov	22.01.2025, 11:59
[sdl-dotnet6] [АНОНС] Кандидат на релиз ASP.NET Core 8.0.12-lvc4-...	• Vlad Efanov	22.01.2025, 11:59
[sdl-dotnet6] [АНОНС] Выпуск релиза .NET8 runtime 8.0.11-lvc3	• Vlad Efanov	24.01.2025, 13:56
[sdl-dotnet6] [АНОНС] Выпуск релиза ASP.NET Core 8.0.11-lvc3	• Vlad Efanov	24.01.2025, 13:56
[sdl-dotnet6] [АНОНС] Выпуск релиза .NET6 runtime 6.0.36-lvc10	• Vlad Efanov	24.01.2025, 13:59
[sdl-dotnet6] [АНОНС] Выпуск релиза ASP.NET Core 6.0.36-lvc10	• Vlad Efanov	24.01.2025, 13:59
[sdl-python3] [АНОНС] Выпуск релиза Python 3.9.21-lvc5	• Vlad Efanov	27.01.2025, 19:30
[sdl-python3] [АНОНС] Выпуск релиза Python 3.10.16-lvc4	• Vlad Efanov	27.01.2025, 19:31
[sdl-python3] [АНОНС] Выпуск релиза Python 3.11.11-lvc5	• Vlad Efanov	27.01.2025, 19:31
[sdl-python3] [АНОНС] Выпуск релиза Python 3.12.8-lvc5	• Vlad Efanov	27.01.2025, 19:32
[sdl-qemu] [АНОНС] Выпуск релиза Qemu 7.2.15-lvc3	• Vlad Efanov	31.01.2025, 14:51
[sdl-dotnet6] [АНОНС] Выпуск релиза .NET8 runtime 8.0.12-lvc4	• Vlad Efanov	13:30
[sdl-dotnet6] [АНОНС] Выпуск релиза ASP.NET Core 8.0.12-lvc4	• Vlad Efanov	13:31

Поддерживаются lvc-ветки компонентов

.NET Runtime 8.0.12-lvc4

Список основных изменений:

1. В качестве базовой версии .NET runtime 8.0 международного сообщества используется версия 8.0.12 (вместо 8.0.11).

В результате обновления до версии 8.0.12 были исправлены следующие уязвимости:

BDU:2025-00367 (CVE-2025-21172) | .NET and Visual Studio Remote Code Execution Vulnerability | Уровень опасности: 7.5 Уязвимость программной платформы Microsoft .NET и средства разработки программного обеспечения Microsoft Visual Studio связана с переполнением буфера в динамической памяти.

Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

BDU:2025-00356 (CVE-2025-21173) | .NET Elevation of Privilege Vulnerability | Уровень опасности: 7.3 Уязвимость программной платформы Microsoft .NET и средства разработки программного обеспечения Microsoft Visual Studio связана с созданием временного файла в каталоге с неправильными разрешениями.

Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

BDU:2025-00588 (CVE-2025-21176) | .NET and Visual Studio Remote Code Execution Vulnerability | Уровень опасности: 8.8 Уязвимость программной платформы Microsoft .NET и средства разработки программного обеспечения Microsoft Visual Studio связана с переполнением буфера в динамической памяти.

Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Дополнительные изменения 8.0.12-lvc4 от 8.0.12, перенесенные из 8.0.11-lvc3:

1. Добавлен патч "fix IndexOutOfRangeException in ZipArchive ", подготовленный Петром Змановским, ООО "БИЗон". Патч устраняет генерацию недокументированного исключения.
2. Добавлен патч " Fix: SafeBerHandle and HGlobalMemHandle leaks in BerConverter (#106316)", подготовленный Александром Хухлаевым, АО "НИКИРЭТ". Патч устраняет потенциальную утечку дескрипторов.
3. Добавлен патч "Fix: resources leak in ActiveDirectorySchemaClass in GetPropertyValuesRecursively", подготовленный Александром Хухлаевым, АО "НИКИРЭТ". Патч устраняет потенциальную утечку ресурсов в ActiveDirectorySchemaClass.
4. Добавлен патч "Fixed: potential null reference in XmlTreeGen when DataSet not defined", подготовленный Сергеем Строниным, АО "Аладдин Р.Д.". Патч устраняет потенциальное разыменование нулевого указателя. (патч не был принят в апстрим).
5. Добавлен патч "Fixed: potential AV in MethodTableBuilder::FindDeclMethodOnClassInHierarchy", подготовленный Сергеем Строниным, АО "Аладдин Р.Д.". Патч устраняет потенциальное разыменование нулевого указателя.

Настоящее

- Системные компоненты
 - поддерживаются lvs-ветки компонентов
 - **настроены процессы автоматического анализа**
 - **статический анализ**
 - **функциональное тестирование**
 - **фаззинг-тестирование**

Выявленные уязвимости

1	LVC-2024-00005	6.2 Средний	Уязвимость функции iso_to_ymd() интерпретатора языка программирования Python3, позволяющая нарушителю вызвать отказ в обслуживании.
---	----------------	-------------	---

Описание

1. LVC-2024-00005

Уязвимость функции iso_to_ymd() в модуле Modules/_datetimemodule.c интерпретатора языка программирования Python3 связана с некорректной проверкой входных данных.

Эксплуатация уязвимости может позволить нарушителю, вызвать отказ в обслужи

Уязвимости подвержены следующие версии:

- от 3.11

исследователь: Ефанов Владислав (ИСП РАН)

автор фаззинг-цели:

Леонид Ревякин (Фобос-НТ) в интересах
ООО «Базальт СПО» для 3.9

Уровень опасности: 6.2 Средний

Вектор уязвимости: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Центр исследований безопасности системного программного обеспечения

Бюллетень уязвимостей
от 04 июня 2024 года

По компоненте Apache Directory Server

	LVC-2024-00007	7.5 Высокий	Уязвимость функции treatLengthEndState() apacheds, позволяющая нарушителю вызвать отказ в обслуживании
--	----------------	-------------	--

1. LVC-2024-00007

Уязвимость функции treatLengthEndState() в модуле asn1/ber/src/main/java/org/apache/directory/api/asn1/ber/Asn1Decoder.java apacheds связана с отсутствием контроля вводимых пользователем данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании

Уязвимости подвержены следующие версии:

- до 2.1.7

автор: Леонид Ревякин

ООО «БАЗИС» / ИСП РАН

Уровень опасности: 7.5 Высокий

Вектор уязвимости: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Настроены процессы автоматического анализа

← → ↺ 🏠 <https://issues.apache.org/jira/browse/DIRAPI-403> 110% ... 📌 ☆

📊  APACHE SOFTWARE FOUNDATION <http://www.apache.org/> Dashboards ▾ Projects ▾ Issues ▾ 🔍 Search ? Log In

Directory Client API / DIRAPI-403

OutOfMemory error in Asn1Decoder for LDAP messages

📄 Export ▾

Details

Type:	 Bug	Status:	RESOLVED
Priority:	 Major	Resolution:	Fixed
Affects Version/s:	2.1.6	Fix Version/s:	2.1.7
Labels:	None		

Description

Hi, we have found Out Of Memory error while fuzzing Asn1Decoder for LDAP messages.

Steps to reproduce:

1. Download Apache Directory LDAP API v2.1.6:

```
wget wget https://github.com/apache/directory-ldap-api/archive/refs/tags/2.1.6.tar.gz
tar xf 2.1.6.tar.gz && rm 2.1.6.tar.gz
```

2. Compile the project (we used jdk-11 and mvn-3.9.6):

```
cd directory-ldap-api-2.1.6
mvn clean package
```

3. Get the reproducer:

```
mkdir fuzz && cd fuzz
mv <path/to/reproducer>/OutOfMemoryReproducer.java .
```

People

Assignee:

 Unassigned

Reporter:

 Andrey Slepykh

Votes:

 0 Vote for this issue

Watchers:

 2 Start watching this issue

Dates

Created:

4 days ago 15:03

Updated:

Yesterday 03:11

Resolved:

Yesterday 03:11

```
#!/bin/bash
for i in {1..50}
do
  nc 127.0.0.1 10389 -w 0 < crash
done
```

@,,~t~Кря

Настоящее

- Системные компоненты
 - поддерживаются lvs-ветки компонентов
 - настроены процессы автоматического анализа
 - статический анализ
 - функциональное тестирование
 - фаззинг-тестирование
 - **организован систематический процесс экспертного анализа результатов**
 - **разметка предупреждений статического анализа**
 - **разработка новых фаззинг-целей**
 - **отчёты о результатах анализа достигаемого покрытия**
 - **исправление выявляемых недостатков**

Систематический процесс анализа результатов

SDL Community v2 / Python3 / Python3-org

18-Sprint_2024-07-11	Добавлено распределение задач для восемнадцатой итерации	7 months ago
19-Sprint_2024-07-25	Добавлено распределение задач для девятнадцатой итерации	6 months ago
20-Sprint_2024-08-08	Добавлено распределение задач для двадцатой итерации	6 months ago
21-Sprint_2024-08-22	Добавлено распределение задач для двадцать первой итерации	5 months ago
22-Sprint_2024-09-05	Добавлено распределение задач для двадцать второй итерации	5 months ago
23-Sprint_2024-09-19	Добавлено распределение задач для двадцать третьей итерации	4 months ago
24-Sprint_2024-10-03	Добавлено распределение задач для двадцать четвёртой итерации	4 months ago
25-Sprint_2024-10-17	Добавлено распределение задач для двадцать пятой итерации	3 months ago
26-Sprint_2024-10-31	Добавлено распределение задач для двадцать шестой итерации	3 months ago
27-Sprint_2024-11-14	Добавлено распределение задач для двадцать седьмой итерации	2 months ago
28-Sprint_2024-11-28	Добавлено распределение задач для двадцать восьмой итерации	2 months ago
29-Sprint_2024-12-12	Добавлено распределение задач для двадцать девятой итерации	1 month ago
30-Sprint_2024-12-26	Исправлены неточности в распределение задач тридцатой итерации для...	1 month ago
31-Sprint_2025-01-23	Добавлено распределение задач для тридцать первой итерации	2 weeks ago
32-Sprint_2025-02-06	Добавлено распределение задач для тридцать второй итерации	1 day ago

Систематический процесс анализа результатов

12 февраля 2025 - m9 - openssl

	Всего	В работе	Подтверждено				Won't Fixed				False Positive				Не распределено
			В работе	Сообщено	Исправлено	Всего	Без вериф.	Не согл.	Вериф-но	Всего	Без вериф.	Не согл.	Вериф-но	Всего	
Критичные	35	-	1	-	9	10	-	-	6	6	1	-	18	19	-
Важные	143	1	3	4	6	13	2	2	41	45	1	-	83	84	-
Средние	276	1	14	17	12	43	-	1	170	171	1	1	59	61	-
Низкие	69	-	3	1	8	12	-	-	46	46	1	-	10	11	-
Всего	523	2	21	22	35	78	2	3	263	268	4	1	170	175	-

- 100% предупреждений уровня Критичный, 96% верифицировано
- 99.3% предупреждений уровня Важный, 96% верифицировано
- 99.6% предупреждений уровня Средний, 98% верифицировано
- 100% предупреждений уровня Низкий, 98% верифицировано

12 февраля 2025 - m09 - Qemu/libvirt

	Всего	В работе	Подтверждено				Won't Fixed				False Positive				Не распределено
			В работе	Сообщено	Исправлено	Всего	Без вериф.	Не согл.	Вериф-но	Всего	Без вериф.	Не согл.	Вериф-но	Всего	
Критичные	472	3	8	1	5	14	187	1	56	244	99	3	62	164	47
Важные	1486	44	46	12	38	96	742	-	199	941	178	-	38	216	189
Средние	1549	-	8	7	22	37	593	4	257	854	98	-	128	226	432
Низкие	444	-	-	-	1	1	246	-	52	298	20	-	1	21	124
Всего	3951	47	62	20	66	148	1768	5	564	2337	395	3	229	627	792

- 89% предупреждений уровня Критичный, 29% верифицировано
- 84% предупреждений уровня Важный, 20% верифицировано
- 72% предупреждений уровня Средний, 35% верифицировано
- 72% предупреждений уровня Низкий, 16% верифицировано

Центр исследований безопасности системного ПО

У каждого проекта – своя специфика РБПО и своё сообщество

166

патчей принято
в исходный код
компонентов

Размечено более

15 тыс. предупреждений,

из которых более

2,5 тыс. прошли независимую

кросс-верификацию

Сейчас в работе

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

Lua 30 тыс. строк

>60

организаций ведут
совместную работу над
компонентами



АТЛАС



<https://portal.linuxtesting.ru>

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

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 «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 «Клауд Солюшенс»
- ООО «КНС ГРУПП»
- ООО «Киберпротект»
- ООО «Код Безопасности»
- ООО «Конфидент»
- ООО «Корбит»
- ООО «НПЦ «КСБ»
- АО «МЦСТ»
- ООО «Национальный каталог»
- АО «НИКИРЭТ»
- 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 «РусБИТех-Астра»
- ФГУП «РФЯЦ-ВНИИЭФ»
- ООО «САФИБ»
- АО МВП «Свемел»
- ООО «СОЛАР Секьюрити»
- ООО «С-Терра СиЭсПи»
- ООО «Стройформ»
- АО «НТЦ ИТ РОСА»
- ООО «ТехАргос»
- ООО «ТСС»
- 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»

Настоящее

- Системные компоненты
 - поддерживаются lvs-ветки компонентов
 - настроены процессы автоматического анализа
 - статический анализ
 - функциональное тестирование
 - фаззинг-тестирование
 - организован систематический процесс экспертного анализа результатов
 - разметка предупреждений статического анализа
 - разработка новых фаззинг-целей
 - отчёты о результатах анализа достигаемого покрытия
 - исправление выявляемых недостатков
 - сформирован Консорциум
 - Программы исследований

Награждение за наиболее значимый вклад 2024

- **Сергей Штылёв** («Открытая мобильная платформа»), за вклад в подготовку исправлений потенциальных уязвимостей в ядре
- **Илья Гаврилов** («ИнфоТекс»), за вклад в проведение разметки результатов статического анализа ядра
- **Никита Жандарович** («ФИНТЕХ»), за вклад в обработку результатов фаззинг-тестирования ядра
- **Дмитрий Фролов** (МВП «Свемел»), за вклад в подготовку исправлений потенциальных уязвимостей в компонентах с открытым исходным кодом
- **Андрей Тишков** («Аладдин Р.Д.»), за вклад в проведение разметки результатов статического анализа компонентов с открытым исходным кодом
- **Валерий Королёв** («Гарда Технологии»), за вклад в развитие фаззинг-тестирования компонентов с открытым исходным кодом
- **Евгений Дикарев** («ИнфоТекс»), за вклад в организацию совместных исследований безопасности компонентов с открытым исходным кодом
- **Андрей Кузнецов** (НТЦ «Фобос-НТ»), за вклад в организацию совместных исследований безопасности компонентов с открытым исходным кодом



Также награды получили две команды разработчиков: в номинациях «Лучшая командная работа по статическому анализу» (победитель – **«Базальт СПО»**) и «Лучшая командная работа по фаззинг-тестированию» (победитель – **«РусБИТех-Астра»**)

- Трансформация Консорциума
 - совместное исследование безопасности как ядра, так и системных компонентов
 - кластеризация компонентов
 - технический комитет для каждого кластера
 - Координационный совет на уровне всего Консорциума
- Масштабирование
 - включение в совместные исследования безопасности компоненты из ПА
- Формирование типовых рекомендаций по анализу ПА
 - Qemu → usbredir, spice, ...
 - FastAPI → Starlette → ASGI server
 - ...

Заключение

- Повышение качества исследования безопасности
- Сокращение дублирования работ
- Независимая экспертиза результатов исследований

Спасибо!



Алексей Хорошилов

khoroshilov@ispras.ru

<https://portal.linuxtesting.ru/>

ИСПРАН

Институт системного программирования им. В.П. Иванникова РАН