

# *Вопросы безопасности заимствованных программных компонентов с открытым исходным кодом*



Алексей Хорошилов  
khoroshilov@ispras.ru



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

# Формирование ИТ-продуктов: как это происходит сейчас в мире



# Уровни зрелости заимствования

- 0. Github, DockerHub, pip, npm, nuget, ...
  - install и забыл

# Уровни зрелости заимствования

- 0. Github, DockerHub, pip, npm, nuget, ...
  - install и забыл
  - install и иногда обновил

# Уровни зрелости заимствования

- 0. Github, DockerHub, pip, npm, nuget, ...
  - install и забыл
  - install и иногда обновил
- 1. Регулярный композиционный анализ
  - каталогизация заимствований
  - реакция на публикацию уязвимостей в заимствованных компонентах

# Уровни зрелости заимствования

- 2. Проверка обновлений доступными средствами
  - сверка идентичности обновлений безопасности (T001)
  - проверка подлинности обновлений безопасности (T002)
  - антивирусный контроль обновлений безопасности (T003)
  - поиск опасных конструкций в обновлениях безопасности (T004)
  - мониторинг активности обновлений безопасности в среде функционирования (T005)

# Уровни зрелости заимствования

- 3. РБПО-практики (SDL, SAST/DAST)
  - статический анализ
  - функциональное тестирование
  - фаззинг-тестирование
- 3а. К обновлениям заимствованных компонентов
- 3б. систематическая проверка всего кода компонентов

# Уровни зрелости заимствования

- 0. Github, DockerHub, pip, npm, nuget, ...
  - install и забыл
  - install и иногда обновил
- 1. Регулярный композиционный анализ
  - каталогизация заимствований
  - реакция на публикацию уязвимостей в заимствованных компонентах
- 2. Проверка обновлений доступными средствами
- 3. РБПО-практики

# Центр исследований безопасности системного программного обеспечения

- Технологический центр исследования безопасности ядра Linux
- Инфраструктура для систематического исследования безопасности критичных компонентов

<https://portal.linuxtesting.ru>

*Федеральный проект «Информационная безопасность»  
национальной программы «Цифровая экономика Российской Федерации»,  
Техническое задание, утверждённое ФСТЭК России*

# Схема взаимодействия Центра

## Центр исследований безопасности системного ПО



# Основные принципы Центра

- Репозиторий с исходным кодом целевого компонента
  - Зеркалирование веток международного сообщества
  - Ветки с дополнительными исправлениями
    - в крайнем случае
    - на период неразглашения
- Настройка процессов автоматического анализа
  - статический анализ (SVACE)
  - фаззинг-тестирование (AFL++, LibFuzzer, ИСП Crusher, syzkaller)
  - функциональное тестирование
- Регрессионный анализ обновлений
- Систематический процесс экспертного анализа результатов
  - двухнедельные итерации
  - разметка предупреждений статического анализа
    - + кросс-верификация
  - разбор падений
  - расширение покрытия функциональными и фаззинг-тестами
- Отслеживание уязвимостей, выявляемых в международном сообществе
- Подготовка рекомендаций по исследованию безопасности компонентов

# Репозиторий с исходным кодом ядра

 **Git repository browser**  
a fast webinterface for the git dscm

index

| Name                               | Description                                                              | Owner                  |
|------------------------------------|--------------------------------------------------------------------------|------------------------|
| <i>LVC</i>                         |                                                                          |                        |
| kernel/git/lvc/linux-stable-rc.git | LVC Linux kernel stable rc tree                                          | LVC                    |
| kernel/git/lvc/linux-stable.git    | LVC Linux kernel stable tree                                             | LVC                    |
| <i>LVC/tools</i>                   |                                                                          |                        |
| tools/lvc/syzkaller.git            | LVC Syzkaller                                                            | LVC                    |
| <i>pub/scm/bluetooth</i>           |                                                                          |                        |
| bluez.git                          | Bluetooth protocol stack for Linux                                       | Marcel Holtmann        |
| sbc.git                            | Bluetooth low-complexity, subband codec (SBC) library                    | Marcel Holtmann        |
| bluetooth-next.git                 | Unnamed repository; edit this file 'description' to name the repository. | grokmirror user        |
| <i>pub/scm/boot</i>                |                                                                          |                        |
| dracut/dracut.git                  | dracut - Initramfs generator using udev                                  | Harald Hoyer           |
| syslinux/syslinux.git              | Unnamed repository; edit this file 'description' to name the repository. | Syslinux workgroup     |
| efilinux/efilinux.git              | The efilinux UEFI boot loader                                            | Matt Fleming           |
| <i>pub/scm/devel</i>               |                                                                          |                        |
| pahole/pahole.git                  | pahole and other type info tools                                         | Arnaldo Carvalho de Me |
| sparse/sparse.git                  | C semantic parser                                                        | Luc Van Oostenryck     |
| sparse/sparse-dev.git              | Sparse's development tree                                                | Luc Van Oostenryck     |
| sparse/sparse-logs.git             | Raw logs of warnings of Sparse running on the kernel with summary logs.  | Luc Van Oostenryck     |
| sparse/chrisl/sparse.git           | Chris Li's sparse repository.                                            | Christopher Li         |
| <i>pub/scm/docs</i>                |                                                                          |                        |
| kernel/pgpkeys.git                 | Kernel developers PGP keys                                               | Kernel.org Admin       |
| docsko/perf.git                    | Unnamed repository; edit this file 'description' to name the repository. | Kernel.org Docs Group  |
| docsko/parisc.git                  | Unnamed repository; edit this file 'description' to name the repository. | Kernel.org Docs Group  |
| kernel/website.git                 | Kernel.org website source                                                | Website Editors        |
| docsko/backports.git               | Unnamed repository; edit this file 'description' to name the repository. | Kernel.org Docs Group  |
| docsko/mtk.git                     | Unnamed repository; edit this file 'description' to name the repository. | Kernel.org Docs Group  |
| docsko/wireless.git                | Unnamed repository; edit this file 'description' to name the repository. | Kernel.org Docs Group  |
| docsko/nvdimms.git                 | Unnamed repository; edit this file 'description' to name the repository. | Kernel.org Docs Group  |

# Репозиторий с исходным кодом ядра



index : kernel/git/lvc/linux-stable.git

linux-5.10-lvc

switch

LVC Linux kernel stable tree

LVC

about **summary** refs log tree commit diff stats

log msg

search

| Branch         | Commit message                                                | Author             | Age     |
|----------------|---------------------------------------------------------------|--------------------|---------|
| linux-6.1-lvc  | PCI: keystone: Fix if-statement expression in ks_pcie_quirk() | Dan Carpenter      | 10 days |
| linux-5.10-lvc | rtlwifi: rtl8192de: fix ofdm power compensation               | Ping-Ke Shih       | 11 days |
| linux-6.1.y    | Linux 6.1.112                                                 | Greg Kroah-Hartman | 2 weeks |
| linux-5.10.y   | Linux 5.10.226                                                | Greg Kroah-Hartman | 5 weeks |

| Tag             | Download                                                              | Author             | Age     |
|-----------------|-----------------------------------------------------------------------|--------------------|---------|
| v6.1.112-lvc5   | linux-stable-6.1.112-lvc5.tar.gz linux-stable-6.1.112-lvc5.tar.xz     | Alexey Khoroshilov | 5 days  |
| v5.10.226-lvc33 | linux-stable-5.10.226-lvc33.tar.gz linux-stable-5.10.226-lvc33.tar.xz | Alexey Khoroshilov | 5 days  |
| v6.1.111-lvc4   | linux-stable-6.1.111-lvc4.tar.gz linux-stable-6.1.111-lvc4.tar.xz     | Alexey Khoroshilov | 14 days |
| v5.10.226-lvc32 | linux-stable-5.10.226-lvc32.tar.gz linux-stable-5.10.226-lvc32.tar.xz | Alexey Khoroshilov | 14 days |
| v6.1.112        | linux-stable-6.1.112.tar.gz linux-stable-6.1.112.tar.xz               | Greg Kroah-Hartman | 2 weeks |
| v6.1.111        | linux-stable-6.1.111.tar.gz linux-stable-6.1.111.tar.xz               | Greg Kroah-Hartman | 4 weeks |
| v5.10.225-lvc31 | linux-stable-5.10.225-lvc31.tar.gz linux-stable-5.10.225-lvc31.tar.xz | Alexey Khoroshilov | 4 weeks |
| v6.1.110        | linux-stable-6.1.110.tar.gz linux-stable-6.1.110.tar.xz               | Greg Kroah-Hartman | 5 weeks |
| v5.10.226       | linux-stable-5.10.226.tar.gz linux-stable-5.10.226.tar.xz             | Greg Kroah-Hartman | 5 weeks |
| v6.1.108-lvc3   | linux-stable-6.1.108-lvc3.tar.gz linux-stable-6.1.108-lvc3.tar.xz     | Alexey Khoroshilov | 5 weeks |
| [...]           |                                                                       |                    |         |

| Age     | Commit message                                                                                           | Author              | Files | Lines   |
|---------|----------------------------------------------------------------------------------------------------------|---------------------|-------|---------|
| 11 days | rtlwifi: rtl8192de: fix ofdm power compensation <b>HEAD</b> <b>v5.10.226-lvc33</b> <b>linux-5.10-lvc</b> | Ping-Ke Shih        | 1     | -6/+7   |
| 11 days | crypto: safexcel - Add error handling for dma_map_sg() calls                                             | Nikita Zhandarovich | 1     | -8/+11  |
| 11 days | crypto: inside_secure - Avoid dma map if size is zero                                                    | Peter Harliman Liem | 1     | -13/+31 |
| 11 days | RDMA/i40iw: Fix potential NULL-ptr-dereference                                                           | Nikita Zhandarovich | 1     | -0/+2   |
| 11 days | wifi: mac80211: add missing NULL check in ieee80211_chswitch_work()                                      | Nikita Zhandarovich | 1     | -0/+3   |
| 11 days | leds: spi-byte: fix usage of child device node before initialization                                     | Fedor Pchelkin      | 1     | -1/+1   |
| 11 days | xfs: journal geometry is not properly bounds checked                                                     | Dave Chinner        | 2     | -33/+70 |
| 11 days | selinux: prevent KMSAN warning in selinux_inet_conn_request()                                            | Andrew Kanner       | 1     | -0/+1   |
| 11 days | scsi: sr: Fix sshdr use in sr_get_events                                                                 | Mike Christie       | 1     | -1/+2   |
| 11 days | sata_dwc_460ex: Fix missing check in sata_dwc_isr                                                        | Dinghao Liu         | 1     | -0/+10  |
| [...]   |                                                                                                          |                     |       |         |

# Основные принципы Центра

- Репозиторий с исходным кодом целевого компонента
  - Зеркалирование веток международного сообщества
  - Ветки с дополнительными исправлениями
    - в крайнем случае
    - на период неразглашения
- Настройка процессов автоматического анализа
  - статический анализ (SVACE)
  - фаззинг-тестирование (AFL++, LibFuzzer, ИСП Crusher, syzkaller)
  - функциональное тестирование
- Регрессионный анализ обновлений
- Систематический процесс экспертного анализа результатов
  - двухнедельные итерации
  - разметка предупреждений статического анализа
    - + кросс-верификация
  - разбор падений
  - расширение покрытия функциональными и фаззинг-тестами
- Отслеживание уязвимостей, выявляемых в международном сообществе
- Подготовка рекомендаций по исследованию безопасности компонентов

# Настройка процессов автоматического анализа

Pipeline Needs Jobs 2 Tests 0

Generate\_configs

Trigger\_kernel\_pipeline

Downstream

✓ configure ↺

✓ compile

✓ compile  
#6668  
Child

Config

✓ linux-6.1.107-lvc2p\_configure\_allmodconfig+com... ↺

✓ linux-6.1.107-lvc2p\_configure\_tinyconfig ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

✓ linux-6.1.107-lvc2p\_configure\_x86\_64\_defconfig... ↺

Build

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+np1008i ↺

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+x86\_kvm... ↺

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+x86\_kvm... ↺

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+x86\_kvm... ↺

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+x86\_kvm... ↺

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+x86\_kvm... ↺

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+x86\_kvm... ↺

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+x86\_kvm... ↺

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+x86\_kvm... ↺

✓ linux-6.1.107-lvc2p\_x86\_64\_defconfig+x86\_kvm... ↺

Svace

✓ linux-6.1.107-lvc2p\_svace\_allmodconfig ↺

✓ linux-6.1.107-lvc2p\_svace\_tinyconfig ↺

Open

Created 12 hours ago by



issues\_token

Maintainer

Close issue



# Svace results (m05) for Linux 5.10.225-rc1(ee485) allmodconfig+compile-test x86\_64-gcc-10



## General

- Version: Linux 5.10.225-rc1(ee485)
- Configuration: allmodconfig+compile-test
- Machine: x86\_64-gcc-10
- Methodics: m05
- Date: 2024-09-02 05:19:13

## Statistics (compared to 5.10.224)

- [New issues: 10, without review: 10](#)
- [Missing issues: 14, without review: 10](#)
- [Modified issues: 894, without review: 648](#)
- [Matched issues: 35117, without review: 27969](#)
- Total issues: 36021, without review: 28627

## Links

- [Link to the job](#)
- [Link to the new results \(Linux 5.10.225-rc1\(ee485\)\)](#)
- [Link to the previous stable results \(Linux 5.10.224\)](#)



Alexey Khoroshilov

5 Feb 11:40 a.m.

New subject: [PATCH 5.10 12/25] drm/vc4: hdmi: Make sure the device is powered with CEC

On 04.02.2022 12:20, Greg Kroah-Hartman wrote:

...

The patch has moved initialization of val local variable into if (enable) branch. But the variable is used in in the else branch as well. As a result we write of its initialized value here:

```
HDMI_WRITE(HDMI_CEC_CNTRL_5, val |  
            VC4_HDMI_CEC_TX_SW_RESET | VC4_HDMI_CEC_RX_SW_RESET);
```

Found by Linux Verification Center (linuxtesting.org) with SVACE.

```
static  
int vc4_hdmi_cec_adap_enable(struct cec_adapter *adap, bool enable)  
{  
    struct vc4_hdmi *vc4_hdmi = cec_get_drvdata(adap);  
    /* clock period in microseconds */  
    const u32 usecs = 1000000 / CEC_CLOCK_FREQ;  
    u32 val;  
    int ret;
```

It seems something is seriously broken in this release.

There are patches already applied in 5.10.202 that are in 5.10.203-rc3 transformed in some strange way, e.g.

Neil Armstrong <narmstrong@baylibre.com>

tty: serial: meson: retrieve port FIFO size from DT

commit 980c3135f1ae6fe686a70c8ba78eb1bb4bde3060 in 5.10.202

```
diff --git a/drivers/tty/serial/meson_uart.c
b/drivers/tty/serial/meson_uart.c
index d06653493f0e..78bda91a6bf1 100644
--- a/drivers/tty/serial/meson_uart.c
+++ b/drivers/tty/serial/meson_uart.c
@@ -728,6 +728,7 @@ static int meson_uart_probe(struct platform_device
*pdev)
{
    struct resource *res_mem, *res_irq;
    struct uart_port *port;
+   u32 fifosize = 64; /* Default is 64, 128 for EE UART_0 */
    int ret = 0;

    if (pdev->dev.of_node)
@@ -755,6 +756,8 @@ static int meson_uart_probe(struct platform_device
*pdev)
    if (!res_irq)
        return -ENODEV;

+   of_property_read_u32(pdev->dev.of_node, "fifo-size", &fifosize);
+
    if (meson_ports[pdev->id]) {
        dev_err(&pdev->dev, "port %d already allocated\n",
    ...
```

- 
- **Subject:** Re: [PATCH 5.10 004/317] r8169: Fix possible ring buffer corruption on fragmented Tx packets.
  - **From:** Alexey Khoroshilov <khoroshilov@xxxxxxxx>
  - **Date:** Thu, 13 Jun 2024 20:21:52 +0300
  - **Cc:** patches@xxxxxxxxxxxxx, Ken Milmore <ken.milmore@xxxxxxxx>, Heiner Kallweit <hkallweit1@xxxxxxxx>, Paolo Abeni <pabeni@xxxxxxxx>, "lvc-project@xxxxxxxxxxxxx" <lvc-project@xxxxxxxxxxxxx>
  - **In-reply-to:** <[20240613113247.702462647@linuxfoundation.org](mailto:20240613113247.702462647@linuxfoundation.org)>
  - **User-agent:** Mozilla/5.0 (X11; Linux x86\_64; rv:68.0) Gecko/20100101 Thunderbird/68.10.0
- 

On 13.06.2024 14:30, Greg Kroah-Hartman wrote:  
> 5.10-stable review patch. If anyone has any objections, please let me know.

The patch is cleanly applied to 5.10, but it leads to uninit value access in rtl\_tx\_slots\_avail().

```
unsigned int frags;
u32 opts[2];

txd_first = tp->TxDescArray + entry;

if (unlikely(!rtl_tx_slots_avail(tp, frags))) {
    ^^^^ - USE OF UNINIT VALUE
    if (net_ratelimit())
        netdev_err(dev, "BUG! Tx Ring full when queue awake!\n");
    goto err_stop_0;
}

opts[1] = rtl8169_tx_vlan_tag(skb);
opts[0] = 0;

if (!rtl_chip_supports_csum_v2(tp))
    rtl8169_tso_csum_v1(skb, opts);
else if (!rtl8169_tso_csum_v2(tp, skb, opts))
    goto err_dma_0;

if (unlikely(rtl8169_tx_map(tp, opts, skb_headlen(skb), skb->data,
    entry, false)))
```

# Основные принципы Центра

- Репозиторий с исходным кодом целевого компонента
  - Зеркалирование веток международного сообщества
  - Ветки с дополнительными исправлениями
    - в крайнем случае
    - на период неразглашения
- Настройка процессов автоматического анализа
  - статический анализ (SVACE)
  - фаззинг-тестирование (AFL++, LibFuzzer, ИСП Crusher, syzkaller)
  - функциональное тестирование
- Регрессионный анализ обновлений
- Систематический процесс экспертного анализа результатов
  - двухнедельные итерации
  - разметка предупреждений статического анализа
    - + кросс-верификация
  - разбор падений
  - расширение покрытия функциональными и фаззинг-тестами
- Отслеживание уязвимостей, выявляемых в международном сообществе
- Подготовка рекомендаций по исследованию безопасности компонентов

# Участники Центра

- **АО «Аладдин Р.Д.»**
- **ООО «Айдеко»**
- ГК «Актив»
- **ООО Фирма «АНКАД»**
- ООО «А-Реал Консалтинг»
- АО «АСКОН»
- АО «НТЦ «Атлас»
- **АО «БАРС Групп»**
- **ООО «Базальт СПО»**
- **ООО «БАЗИС»**
- **ООО «БЕЛЛСОФТ»**
- **ООО «БИЗон»**
- ООО «Веблук»
- **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 «Код Безопасности»**
- **ООО «Конфидент»**
- ООО «Кросстех Солюшнс Групп»
- 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-Вижен»
- **ООО «РЕД СОФТ»**
- **ООО «РусБИТех-Астра»**
- **ФГУП «РФЯЦ-ВНИИЭФ»**
- ООО «САФИБ»
- **АО МВП «Свемел»**
- **ООО «СОЛАР Секьюрити»**
- ООО «Стройформ»
- **ООО «НТЦ ИТ РОСА»**
- **ООО «ТехАргос»**
- 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»**

# Статистика по разметке предупреждений

15 октября 2024 - 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     | 860          | 17         | -            | 42          | 6          | 45         | 4         | -         | 97          | 247         | -           | 271          | 518          | 73             | -           | 155          | 228         |
| 02-basealt      | 630          | -          | -            | 52          | -          | 10         | 3         | -         | 65          | 192         | -           | 340          | 532          | 8              | -           | 25           | 33          |
| 03-astralinux   | 660          | -          | -            | 23          | 15         | 37         | 17        | 7         | 92          | 181         | -           | 200          | 381          | 71             | -           | 116          | 187         |
| 04-rosa         | 820          | -          | -            | 31          | 12         | 13         | -         | 3         | 59          | 310         | -           | 223          | 533          | 122            | -           | 106          | 228         |
| 05-ivk          | 620          | 1          | 2            | 55          | 5          | 12         | 2         | -         | 76          | 188         | -           | 177          | 365          | 72             | -           | 106          | 178         |
| 06-redsoft      | 860          | -          | -            | 79          | 3          | 24         | 3         | 1         | 110         | 308         | 1           | 222          | 531          | 96             | 1           | 122          | 219         |
| 07-yandex       | 780          | -          | -            | 40          | 8          | 11         | 6         | 3         | 67          | 285         | -           | 196          | 481          | 88             | -           | 144          | 232         |
| 08-aladdin      | 780          | 1          | -            | 100         | 1          | 29         | 5         | 2         | 137         | 342         | -           | 156          | 498          | 32             | -           | 112          | 144         |
| 09-mcst         | 860          | -          | -            | 46          | 17         | 54         | 4         | 1         | 121         | 378         | 2           | 265          | 645          | 31             | -           | 63           | 94          |
| 10-omp          | 660          | -          | -            | 24          | 44         | 65         | 3         | -         | 136         | 171         | -           | 189          | 360          | 65             | -           | 99           | 164         |
| 12-securitycode | 740          | -          | -            | 49          | 9          | 24         | 2         | -         | 84          | 302         | 7           | 190          | 499          | 46             | -           | 111          | 157         |
| 13-infotecs     | 622          | -          | -            | 27          | -          | 20         | 20        | 6         | 67          | 181         | -           | 177          | 358          | 59             | -           | 138          | 197         |
| 14-swemel       | 780          | -          | -            | 12          | 5          | 32         | 4         | 8         | 58          | 383         | -           | 267          | 650          | 8              | -           | 64           | 72          |
| 15-fintech      | 660          | -          | -            | -           | -          | 55         | 35        | 2         | 91          | 216         | -           | 255          | 471          | 17             | -           | 81           | 98          |
| 16-factor-ts    | 270          | 47         | -            | 11          | 10         | 4          | 3         | -         | 28          | 28          | 1           | 102          | 131          | 9              | -           | 55           | 64          |
| 17-confident    | 740          | 2          | 4            | 39          | 1          | 13         | 2         | -         | 59          | 206         | 2           | 180          | 388          | 136            | 3           | 152          | 291         |
| 18-rasu         | 820          | 2          | -            | 29          | -          | 8          | 4         | 1         | 42          | 383         | 10          | 239          | 632          | 58             | 2           | 84           | 144         |
| 19-itb          | 660          | 118        | -            | 118         | -          | 12         | -         | -         | 130         | 115         | -           | 105          | 220          | 87             | -           | 105          | 192         |
| 20-ideco        | 740          | 120        | 14           | 67          | -          | 10         | 1         | -         | 92          | 261         | 14          | 195          | 470          | 17             | -           | 41           | 58          |
| 21-nppct        | 780          | -          | -            | 3           | 6          | 12         | -         | -         | 21          | 350         | -           | 291          | 641          | 37             | -           | 81           | 118         |
| 22-usergate     | 860          | 29         | -            | 40          | 2          | 17         | 2         | 2         | 61          | 401         | 3           | 356          | 760          | 1              | -           | 9            | 10          |
| 23-vniief       | 570          | 4          | 3            | 1           | -          | 1          | -         | -         | 5           | 207         | 3           | 267          | 477          | 44             | -           | 40           | 84          |
| 24-msvsphere    | 620          | 5          | -            | 106         | 4          | 43         | -         | -         | 153         | 154         | 5           | 138          | 297          | 69             | -           | 96           | 165         |
| 25-ancud        | 740          | 25         | 7            | 16          | 5          | 38         | 4         | -         | 70          | 155         | 9           | 253          | 417          | 60             | 7           | 161          | 228         |
| 26-t-argos      | 640          | 107        | -            | 41          | 34         | 34         | 2         | 9         | 118         | 110         | -           | 197          | 307          | 23             | -           | 85           | 108         |
| 27-plc          | 420          | 115        | -            | 30          | -          | -          | -         | -         | 30          | 63          | 2           | 63           | 128          | 77             | 4           | 66           | 147         |
| 28-yadro        | 620          | -          | -            | 40          | 1          | 23         | -         | -         | 64          | 201         | 4           | 242          | 447          | 19             | -           | 90           | 109         |
| 29-maxima       | 220          | 22         | -            | 20          | 3          | 34         | -         | 1         | 58          | 44          | 2           | 82           | 128          | 1              | -           | 11           | 12          |
| <b>Всего:</b>   | <b>19032</b> | <b>615</b> | <b>30</b>    | <b>1141</b> | <b>191</b> | <b>680</b> | <b>46</b> | <b>46</b> | <b>2191</b> | <b>6362</b> | <b>65</b>   | <b>5838</b>  | <b>12265</b> | <b>1426</b>    | <b>17</b>   | <b>2518</b>  | <b>3961</b> |

- 99.7% предупреждений уровня Критичный, 85% верифицировано
- 66.9% предупреждений уровня Важный, 54% верифицировано

# Статистика по принятым исправлениям в ядро

|                                    | Февраль 2023 (105) | Август 2023 (190) | Февраль 2024 (275) | Сентябрь 2024 (416) |
|------------------------------------|--------------------|-------------------|--------------------|---------------------|
| АО «Аладдин Р.Д.»                  | 0                  | 3                 | 5                  | 11                  |
| ООО Фирма «АНКАД»                  | -                  | 0                 | 2                  | 6                   |
| ООО «Базалыт СПО»                  | 1                  | 4                 | 4                  | 4                   |
| ООО «БЕЛЛСОФТ»                     | 7                  | 10                | 10                 | 14                  |
| АО «ИВК»                           | 0                  | 4                 | 4                  | 4                   |
| ООО «Инферит»                      | -                  | 1                 | 17                 | 40                  |
| АО «ИнфоТекС»                      | 3                  | 9                 | 14                 | 16                  |
| ООО «ИТБ»                          | 0                  | 0                 | 1                  | 1                   |
| ООО «Код Безопасности»             | 0                  | 3                 | 3                  | 3                   |
| ООО «Конфидент»                    | 0                  | 0                 | 1                  | 3                   |
| ООО «МТ-Интеграция»                | -                  | -                 | -                  | 1                   |
| АО «МЦСТ»                          | 0                  | 1                 | 1                  | 3                   |
| АО «НППКТ»                         | -                  | -                 | 0                  | 1                   |
| ООО «Открытая мобильная платформа» | 24                 | 27                | 38                 | 51                  |
| АО «РАСУ»                          | 3                  | 4                 | 5                  | 6                   |
| ООО «РЕД СОФТ»                     | 3                  | 5                 | 11                 | 13                  |
| ООО «НТЦ ИТ РОСА»                  | 0                  | 0                 | 0                  | 7                   |
| ООО «РусБИТех-Астра»               | 6                  | 8                 | 13                 | 19                  |
| АО МВП «Свемел»                    | 1                  | 4                 | 7                  | 9                   |
| ООО «ТехАргос»                     | -                  | -                 | 0                  | 28                  |
| ООО «Фактор-ТС»                    | 4                  | 4                 | 4                  | 4                   |
| АО «ФИНТЕХ»                        | 4                  | 20                | 24                 | 34                  |
| ООО «Юзергейт»                     | -                  | 0                 | 0                  | 2                   |
| ООО «ЯНДЕКС.ОБЛАКО»                | 5                  | 10                | 12                 | 13                  |
| Сотрудники центра                  | 44                 | 72                | 99                 | 123                 |

# 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

## ОТЧЁТ О РЕЗУЛЬТАТАХ ВЫПОЛНЕНИЯ ПРОГРАММЫ ИССЛЕДОВАНИЙ

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

Ключевые показатели Программы исследований включали в себя:

- отработка результатов статического анализа в объёме не менее 500 предупреждений (п. 3.3 Программы) в соответствии с требованиями (п. 3.4 Программы):
  - для каждого предупреждения проведён анализ актуальности и присвоена одна из трех меток «Подтверждено», «Не актуально», «Ложное срабатывание» (п. 3.4.2 Программы),
  - для каждого подтвержденного предупреждения выполнена оценка с точки зрения его влияния на безопасность (п. 3.4.3 Программы),
  - для каждого подтвержденного предупреждения, влияющего на безопасность (уровень критичности «Critical» или «Major») и подтверждённого кросс-верификацией (п. 3.4.4 Программы) выполнено исправление;

# Программа исследований №1

Программа исследований до 1 марта 2024 г.

01 апреля 2024

|                 | Участвуют | п. 3.3 (500) + п.4.2(0-120) |          | п.3.4.4 (исправления) | п. 4.1 (публикация) |          | п. 4.2 (фаззинг) |        |          |
|-----------------|-----------|-----------------------------|----------|-----------------------|---------------------|----------|------------------|--------|----------|
|                 |           | Готово                      | Осталось | Осталось              | Готово              | Осталось | В процессе       | Готово | Осталось |
| 01-bellsoft     | Да        | 565                         | 55       | 23                    | 7                   | 3        | -                | -      | -        |
| 02-basealt      | Да        | 496                         | 4        | 0                     | 11                  | 0        | -                | 3      | 0        |
| 03-astralinux   | Да        | 503                         | 0        | 0                     | 15                  | 0        | -                | 4      | 0        |
| 04-rosa         | Да        | 603                         | 17       | 2                     | 0                   | 10       | -                | -      | -        |
| 05-ivk          | Да        | 498                         | 2        | 2                     | 11                  | 0        | -                | 3      | 0        |
| 06-redsoft      | Да        | 616                         | 4        | 6                     | 26                  | 0        | -                | -      | -        |
| 07-yandex       | Да        | 620                         | 0        | 0                     | 35                  | 0        | -                | -      | -        |
| 08-aladdin      | Да        | 580                         | 0        | 2                     | 10                  | 0        | -                | 1      | 0        |
| 09-mcst         | Да        | 618                         | 2        | 6                     | 11                  | 0        | -                | -      | -        |
| 10-omp          | Да        | 540                         | 0        | 0                     | 14                  | 0        | -                | 2      | 0        |
| 12-securitycode | Да        | 591                         | 29       | 6                     | 0                   | 10       | -                | -      | -        |
| 13-infotecs     | Да        | 502                         | 0        | 0                     | 13                  | 0        | -                | 3      | 0        |
| 14-swemel       | Да        | 620                         | 0        | 0                     | 13                  | 0        | -                | -      | -        |
| 15-fintech      | Да        | 540                         | 0        | 0                     | 11                  | 0        | -                | 5      | 0        |
| 17-confident    | Да        | 618                         | 2        | 8                     | 5                   | 5        | -                | -      | -        |
| 18-rasu         | Да        | 620                         | 0        | 0                     | 4                   | 6        | -                | -      | -        |
| 19-itb          | Да        | 511                         | 29       | 5                     | 26                  | 0        | 2                | 0      | 2        |
| 20-ideco        | Да        | 492                         | 8        | 5                     | 0                   | 10       | 0                | 0      | 3        |
| 21-nppct        | Да        | 577                         | 3        | 10                    | 5                   | 5        | -                | 1      | 0        |
| 22-usergate     | Да        | 620                         | 0        | 10                    | 12                  | 0        | -                | -      | -        |
| 24-msvsphere    | Да        | 500                         | 0        | 0                     | 3                   | 7        | -                | 3      | 0        |
| 25-ancud        | Да        | 597                         | 23       | 63                    | 2                   | 8        | -                | -      | -        |
| 26-t-argos      | Да        | 120                         | 380      | 25                    | 7                   | 3        | 0                | 0      | 3        |

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, недеklarированных 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

# Программа исследований №2

Программа исследований до 1 октября 2024 г.

11 октября 2024

|                 | Участвуют | Статический анализ |          | Исправления | Бэкпорт  | Загрузка |          | Фаззинг |          |
|-----------------|-----------|--------------------|----------|-------------|----------|----------|----------|---------|----------|
|                 |           | Готово             | Осталось | Осталось    | Осталось | Готово   | Осталось | Готово  | Осталось |
| 01-bellsoft     | Да        | 220                | 20       | 1           | 0        | 15       | 0        | 0       | 0        |
| 02-basealt      | Да        | 130                | 0        | 0           | 0        | 22       | 0        | 4       | 0        |
| 03-astralinux   | Да        | 160                | 0        | 2           | 0        | 16       | 0        | 2       | 0        |
| 04-rosa         | Да        | 200                | 0        | 1           | 0        | 15       | 0        | 1       | 0        |
| 05-ivk          | Да        | 119                | 1        | 2           | 0        | 22       | 0        | 4       | 0        |
| 06-redsoft      | Да        | 236                | 4        | 8           | 2        | 19       | 0        | 0       | 0        |
| 07-yandex       | Да        | 159                | 1        | 0           | 2        | 16       | 0        | 2       | 0        |
| 08-aladdin      | Да        | 198                | 2        | 0           | 6        | 15       | 0        | 1       | 0        |
| 09-mcst         | Да        | 235                | 5        | 6           | 4        | 17       | 0        | 0       | 0        |
| 10-omp          | Да        | 120                | 0        | 0           | 0        | 16       | 0        | 3       | 0        |
| 12-securitycode | Да        | 110                | 10       | 7           | 7        | 2        | 13       | 0       | 3        |
| 13-infotecs     | Да        | 122                | 0        | 0           | 0        | 15       | 0        | 4       | 0        |
| 14-swemel       | Да        | 160                | 0        | 0           | 1        | 16       | 0        | 3       | 0        |
| 15-fintech      | Да        | 120                | 0        | 0           | 4        | 15       | 0        | 9       | 0        |
| 17-confident    | Да        | 113                | 7        | 10          | 0        | 0        | 15       | 0       | 3        |
| 18-rasu         | Да        | 181                | 19       | 0           | 1        | 12       | 3        | 0       | 1        |
| 19-itb          | Да        | -2                 | 122      | 4           | 2        | 15       | 0        | -2      | 5        |
| 20-ideco        | Да        | -31                | 151      | 20          | 0        | 19       | 0        | 2       | 1        |
| 21-nppct        | Да        | 199                | 1        | 5           | 0        | 23       | 0        | 0       | 1        |
| 22-usergate     | Да        | 206                | 34       | 13          | 7        | 15       | 0        | 0       | 0        |
| 24-msvsphere    | Да        | 109                | 11       | 0           | 0        | 6        | 9        | 5       | 0        |
| 25-ancud        | Да        | 76                 | 44       | 9           | 3        | 14       | 1        | 0       | 3        |
| 26-t-argos      | Да        | -94                | 214      | 37          | 2        | 16       | 0        | 0       | 3        |
| 27-plc          | Да        | -336               | 576      | 0           | 0        | -10      | 25       | 0       | 0        |
| 28-yadro        | Да        | 115                | 5        | 5           | 0        | -4       | 19       | 1       | 2        |
| 29-maxima       | Да        | -302               | 422      | 6           | 0        | -5       | 20       | -3      | 6        |

# 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

100

патчей принято  
в исходный код  
компонентов

## 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



# Заключение

- Повышение зрелости использования заимствованных компонентов
- Сокращение дублирования работ

# Спасибо!



Алексей Хорошилов  
khoroshilov@ispras.ru

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

**ИСПРАН**

Институт системного программирования им. В.П. Иванникова РАН