Технологический центр исследования безопасности ядра Linux и критических компонентов

Алексей Хорошилов
khoroshilov@ispras.ru

ИСП РАН

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

Технологический центр исследования безопасности ядра Linux

- Повышение уровня безопасности отечественных систем на основе ядра Linux
  - систематическое применение лучших практик разработки безопасного ПО
    - статический анализ исходного кода ядра
    - фаззинг-тестирования ядра
    - системное и модульное тестирование
    - архитектурный анализ
    - полносистемный динамический анализ помеченных данных
  - подготовка методик и рекомендаций по реализации мер безопасной разработки для ядра Linux
  - ведение ветки ядра, прошедшей требуемые исследования
  - разработка
    - патчей по устранению уязвимостей и ошибок
    - новых возможностей, нацеленных на повышение безопасности
  - наполнение БДУ ФСТЭК России сведениями об уязвимостях ядра Linux

Текущее состояние

- (1) Ведётся сопровождение ветки ядра, основанной на стабильной версии 5.10
- (2) Подготовлены методики проведения исследования ядра Linux, включая
  - статический анализ при помощи инструмента SVACE
  - системное и модульное тестирование (наполнение тестовыми наборами продолжается)
  - фаззинг-тестирование при помощи инструмента syzkaller
  - проведение архитектурного анализа с целью определения поверхности атаки
  - проведение анализа помеченных (чувствительных) данных
- (3) Создана экспертная группа, состоящая из представителей 19 компаний, в рамках которой
  - формируются принципы функционирования Технологического центра
  - проведена разметка более 4,5 тыс. предупреждений инструмента статического анализа SVACE
  - подготовлен ряд исправлений ошибок в ядре, 48 из которых уже были приняты в основную ветку ядра
- (4) Готовятся рекомендации по конфигурированию ядра с целью повышения его безопасности
- (5) Ведётся доработка исправлений, нацеленных на повышение безопасности работы ядра, на стадии его развёртывания и инициализации

(1) Ветка ядра

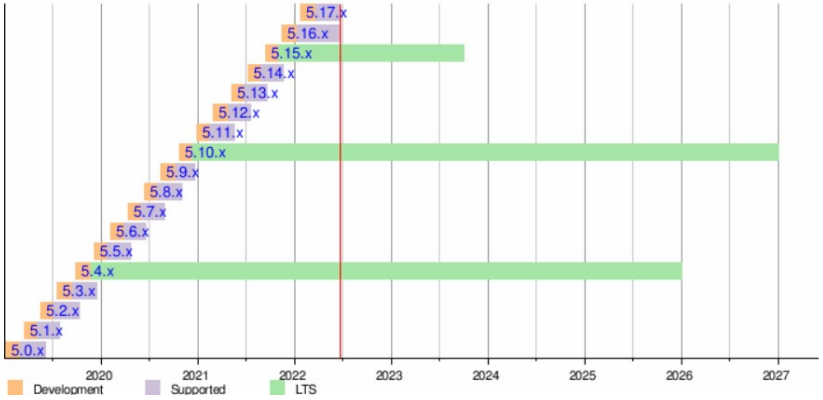
- Ведётся сопровождение ветки ядра, основанной на стабильной версии 5.10

Для доступа к ветке используйте следующие ссылки:

Версия	Дата выпуска	Архив	Подпись	Репозиторий
5.10.139	2022-08-29	[tarball]	[подпись]	[browse]

Инструкция по проверке подписи ядра

- Анализ новых предупреждений SVACE
- Выполнение тестовых наборов
- Фаззинг-тестирование (до появления следующей версии)
- Экспертная оценка патчей



(2) Методики проведения исследования ядра

- статический анализ при помощи инструмента SVACE
  - методика версии m03 на основе SVACE-3.3.0
- системное и модульное тестирование
  - наполнение тестовыми наборами продолжается
- фаззинг-тестирование при помощи инструмента syzkaller
- проведение архитектурного анализа с целью определения поверхности атаки
- проведение анализа помеченных (чувствительных) данных

(2) Методики проведения исследования ядра

- статический анализ при помощи инструмента SVACE
  - методика версии m03 на основе SVACE-3.3.0
  - двухнедельные итерации по разметке предупреждений
    - 15-20 предупреждений на организацию
    - 275-300 предупреждений за итерацию

m03	10 июня 2022				11 июля 2022				19 августа 2022		
	В работе	Обработано	Всего		В работе	Обработано	Всего		В работе	Обработано	Всего
Критичные	1767	44 (2%)	1811		928	892 (49%)	1820		312	1508 (83%)	1820
Важные	14582	1296 (8%)	15878		14121	1666 (11%)	15787		13822	1978 (12%)	15800
Средние	3268	78 (2%)	3346		3294	85 (2%)	3379		3223	156 (4%)	3379
Низкие	12086	386 (3%)	12472		12081	412 (3%)	12493		12033	470 (3%)	12503
Всего	**31703**	**1804 (5%)**	**33507**		**30424**	**3055 (9%)**	**33479**		**29390**	**4112 (12%)**	**33502**

(3) Партнёры Технологического центра

- формируются принципы функционирования Технологического центра
- проведена разметка более 4 тыс. предупреждений инструмента статического анализа SVACE
- подготовлен ряд исправлений ошибок в ядре, 48 из которых уже приняты в основную ветку ядра

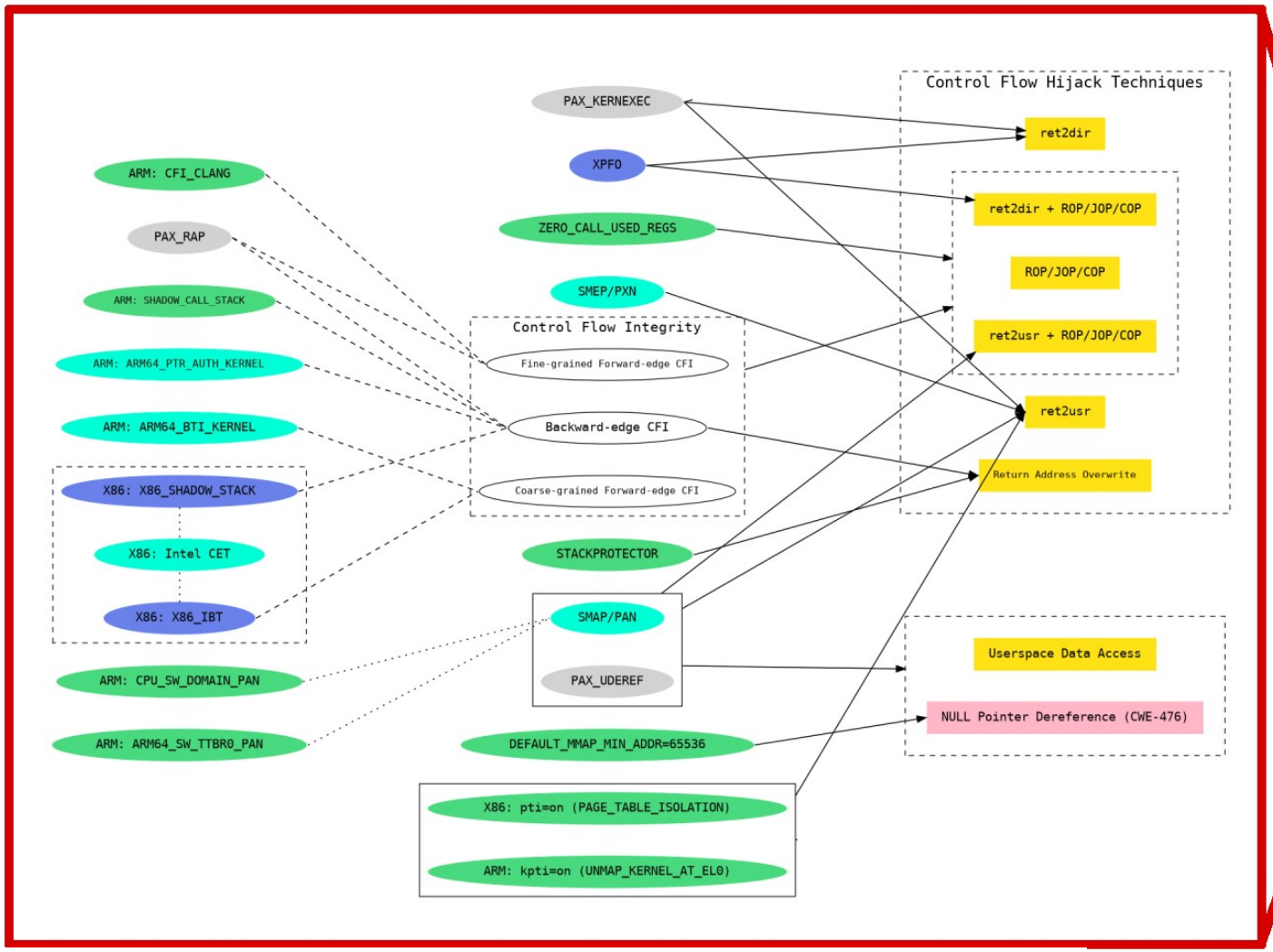
Date range	1-bellsoft	10-omp		12-securitycode		13-infotecs	14-swemel	15-fintech			2-basealt	3-astralinux	4-rosa		5-ivk	6-redsoft	7-yandex		8-aladdin	9-mcst	
	aleksei.kodanev	k.yankevich	shtylyov	i.kapranov	sapozhnikov	ilia.gavrilov	arefev	loshkarev	n.petrova	rusakov	gremlin	vtelezhnikov	d.anisimov	v.ryabokon	burdovitsyn	anton.fadeev	arbn	d-tatianin	d.dulov98	artemiev	iarapov
12 May, 2022 - 19 May, 2022	5	-	7	-	-	40	-	-	-	-	-	9	-	-	-	-	-	-	-	-	-
19 May, 2022 - 26 May, 2022	3	-	2	-	-	3	-	-	-	-	-	7	-	-	-	-	-	-	19	-	-
26 May, 2022 - 02 Jun, 2022	10	6	7	-	9	61	-	-	-	-	3	18	6	-	15	10	-	-	17	-	3
02 Jun, 2022 - 09 Jun, 2022	21	-	2	5	16	27	-	-	-	-	18	11	6	-	23	14	-	33	12	-	25
09 Jun, 2022 - 16 Jun, 2022	13	7	5	10	10	13	-	-	-	-	17	4	3	-	2	-	-	-	12	-	27
16 Jun, 2022 - 23 Jun, 2022	2	7	6	6	-	9	-	-	-	-	5	1	35	-	10	-	-	17	-	-	12
23 Jun, 2022 - 30 Jun, 2022	-	2	8	6	8	13	-	-	-	-	27	-	-	-	2	3	-	-	17	-	15
30 Jun, 2022 - 07 Jul, 2022	15	-	7	7	-	5	-	-	-	-	-	36	14	-	20	21	16	-	14	-	-
07 Jul, 2022 - 14 Jul, 2022	23	1	14	1	-	-	-	-	-	-	-	-	1	1	10	-	-	-	12	-	4
14 Jul, 2022 - 21 Jul, 2022	-	-	3	-	-	-	-	-	-	-	19	15	-	15	15	8	12	-	-	11	-
21 Jul, 2022 - 28 Jul, 2022	4	-	6	-	23	37	11	-	-	-	19	3	-	11	-	13	12	13	15	24	-
28 Jul, 2022 - 04 Aug, 2022	25	-	7	-	-	25	17	5	82	1	-	15	-	4	15	2	-	-	-	8	-
04 Aug, 2022 - 11 Aug, 2022	6	-	1	6	-	73	15	-	6	2	13	2	-	1	15	-	-	-	13	18	-
11 Aug, 2022 - 13 Aug, 2022	6	-	-	3	-	13	2	-	-	-	-	-	-	-	3	-	-	7	-	-	-
Total	105	21	75	37	57	286	35	5	83	1	102	105	59	32	112	65	30	70	90	48	69

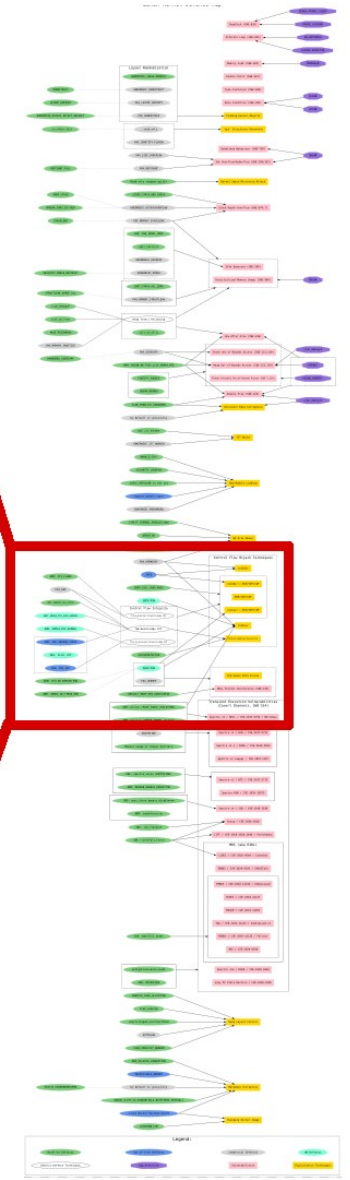
(3) Партнёры Технологического центра

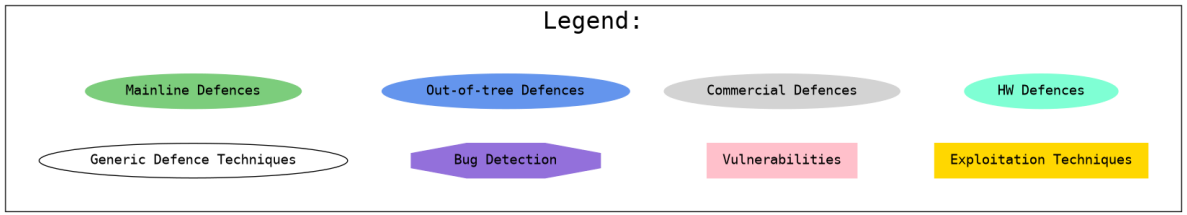
- АО «Аладдин Р.Д.»
- ООО «Базальт СПО»
- АО «Байкал электроникс»
- ООО «БЕЛЛСОФТ»
- АО «ИВК»
- АО «ИнфоТеКС»
- ООО «Код Безопасности»
- ООО «Конфидент»
- АО НТЦ «Модуль»
- АО «МЦСТ»
- ООО «Открытая мобильная платформа»
- АО «РАСУ»
- ООО «РЕД СОФТ»
- ООО «РусБИТех-Астра»
- АО МВП «Свемел»
- ООО «НТЦ ИТ РОСА»
- ООО «Фактор-ТС»
- АО «ФИНТЕХ»
- ООО «ЯНДЕКС.ОБЛАКО»

(4) Карта средств защиты ядра

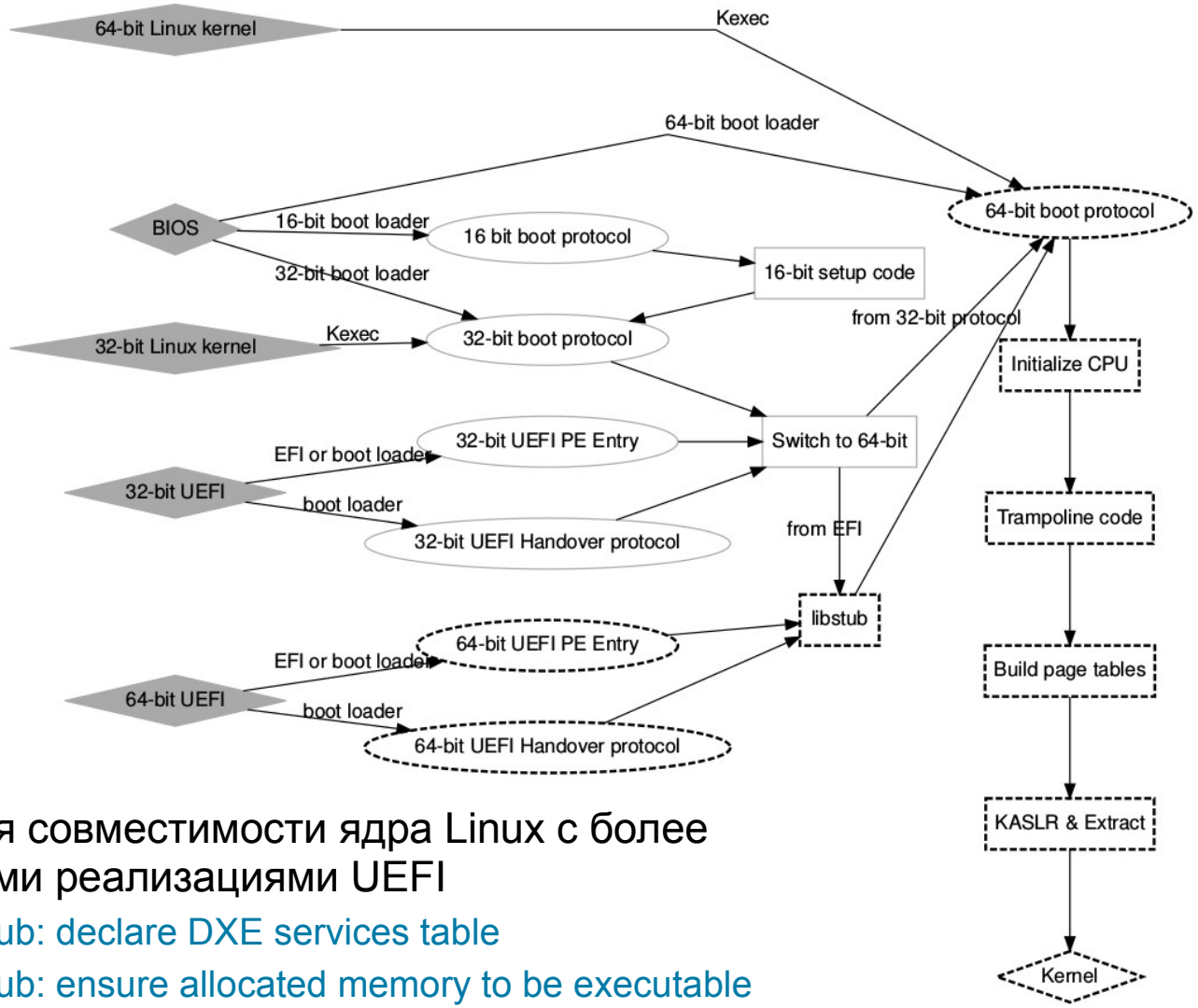
https://github.com/a13xp0p0v/linux-kernel-defence-map







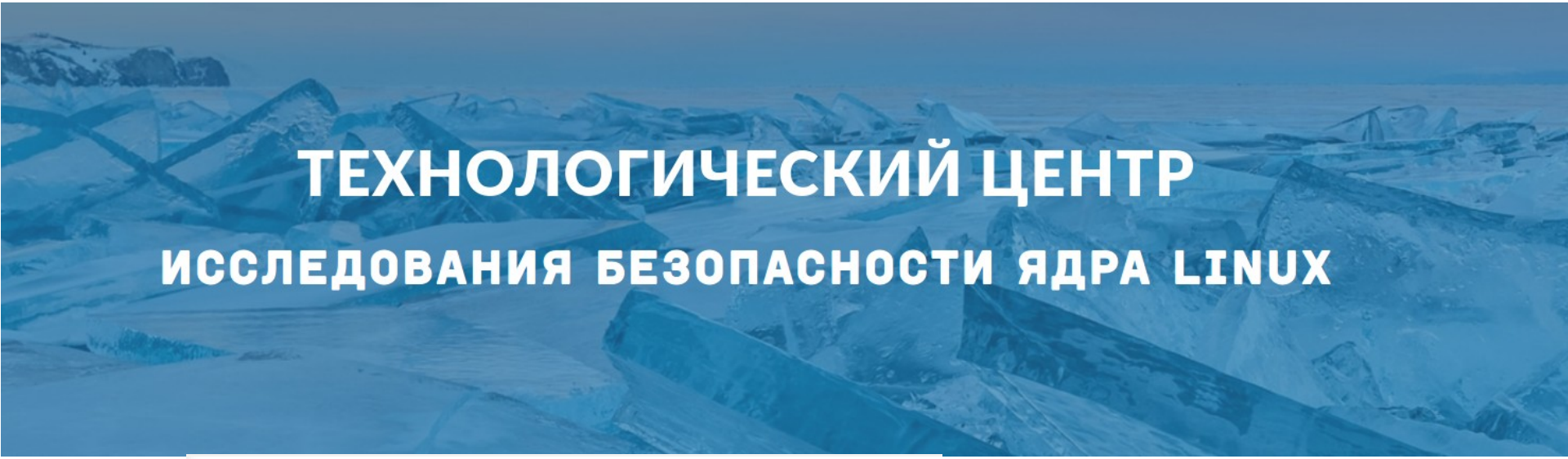
(5) Доработки в ядре



- Реализация совместимости ядра Linux с более безопасными реализациями UEFI
  - efi: libstub: declare DXE services table
  - efi: libstub: ensure allocated memory to be executable
- Повышение безопасности ядра Linux на ранних этапах загрузки (в работе)

Веб-портал Технологического центра

https://portal.linuxtesting.ru



Ближайшие планы

- Разметка всех предупреждений уровня **Критичный**
- Развитие методик
  - расширение покрытия тестами и фаззинг-тестированием
- Внедрение методик в процессы сертификационных испытаний
- Формирование соглашения о партнёрстве и меморандума
  - Подключение новых партнёров
  - Приглашаем все заинтересованные компании!
- Рабочая группа по обеспечению безопасной загрузки Linux

Инфраструктура исследования безопасности критичных компонентов

- Сбор статистики по компонентам
  - Предварительный сбор данных:
    - см. ссылку в @sdl_community
  - Машиночитаемый формат описания заимствованных компонентов
- Отладка процессов ведётся в рамках сообщества:
  - Телеграмм канал @sdl_community
  - https://gitlab.community.ispras.ru/
  - на примере Node.js, .Net, Lua, EDKII и др.

Организация	
АО «Аладдин Р.Д.»	3
ООО «Айдеко»	3
ООО «Гарда Технологии»	4
АО «ИнфоТеКС»	1
ООО «Код Безопасности»	7
ООО «Конфидент»	2
ООО «КНС ГРУПП» (YADRO)	5
АО «Лаборатория Касперского»	7
ООО «НПЦ КСБ»	5
ООО «Р-Вижн»	1
ООО «РусБИТех-Астра»	1
ООО «САФИБ»	1
ООО НТЦ «Фобос-НТ»	2

Инфраструктура исследования безопасности критичных компонентов

- nodejs
- LUA
- ASP .NET Core
- .NET Core
- .NET
- IdentityServer4
- Django
- Nginx
- dropbear
- BusyBox
- suricata
- python
- ntp
- nxlog
- pacemaker
- squid
- Go
- gRPC (Go)
- protobuf
- OpenSSL
- Qt
- minizip
- tinyxml
- zlib
- lzmalib
- libmariadb
- clucene
- boost
- libreoffice
- re2
- linux-pam

Заключение

- Разрабатывая свои продукты
  - Определите заимствованные компоненты, находящиеся на поверхности атаки
  - Оцените исследование каких компонентов предпочтительно вести самостоятельно, а каких совместно
  - Присоединяйтесь к сообществу!

LinuxTesting.org

Спасибо!

Алексей Хорошилов
khoroshilov@ispras.ru
https://portal.linuxtesting.ru/

ИСП РАН
Институт системного программирования им. В.П. Иванникова РАН