



2026

ОС Astra Linux: нам по пути с РБПО

Тележников Владимир
Директор департамента
анализа безопасности, к.т.н.

Управление уязвимостями

Комплексный подход: в 2025 году

>47 000 (+39%)

проанализировано уязвимостей (CVE)

>11 000 (+93%)

паспортов уязвимостей (CVE) отправлено в БДУ ФСТЭК России

>70 (+96%)

паспортов уязвимостей (ASE) отправлено в БДУ ФСТЭК России

Паспорта Приоритизация УБИ Архитектура и модель угроз Трекер задач Продукты ГК

python

+ Добавить запись

Пакет	Поверхность атаки	Интерпретатор	ФБ	Релиз	Действия
python3.11	Поверхность атаки	✓	ФБ.00: Обеспечение ФБ	1.8_main 3.8_main	✎ 🗑 📄
python3.7	Поверхность атаки	✓	ФБ.00: Обеспечение ФБ	1.7_main 4.7_main	✎ 🗑 📄
dnspython	Косвенная поверхность атаки	✗	ФБ.00: Обеспечение ФБ	1.6_main 1.7_main 1.8_main 3.8_main 4.7_main 8.1_main	✎ 🗑 📄
python-gssapi	Косвенная поверхность атаки	✗	ФБ.00: Обеспечение ФБ	1.6_main 1.7_main 1.8_main 3.8_main 4.7_main 8.1_main	✎ 🗑 📄
python-ldap	Косвенная поверхность атаки	✗	ФБ.00: Обеспечение ФБ	1.6_main 1.7_main 1.8_main 3.8_main 4.7_main 8.1_main	✎ 🗑 📄
python-urllib3	Косвенная поверхность атаки	✗	ФБ.00: Обеспечение ФБ	1.6_main 1.7_main 1.8_main 3.8_main 4.7_main 8.1_main	✎ 🗑 📄
dbus-python	Не относится к ПА	✗	ФБ.00: Обеспечение ФБ	1.6_main 1.7_main 1.8_main 3.8_main 4.7_main 8.1_main	✎ 🗑 📄

Строк на страницу 100 1-100 of 495

Управление уязвимостями

Контроль зависимостей

>4 000

компонентов ОС покрывается непрерывным SCA

>20

выпусков обновлений ОС и продуктов экосистемы сопровождались отправкой SBOM во ФСТЭК России

>10

продуктов экосистемы проектируются с учетом SBOM ОС

The screenshot displays the PATCH CHECKER web application interface. The main area shows the process of generating an SBOM for 'Astra Linux Special Edition 1.8'. The interface includes a sidebar with navigation options like 'Главная страница', 'Поиск CVE', and 'Аналитика'. The main content area has tabs for 'Готовые', 'Отправленные', 'Ошибки', and 'Логи по SBOM'. Below these are buttons for 'Генерация хеша', 'Обогатить SBOM', 'Проверить SBOM', and 'Создать SBOM'. The 'Создать SBOM' button is highlighted in red. Below the main content area, there is a 'JSON отчет' section showing details for a report with ID 19, including the report name 'Astra_Linux_Special_Edition_1.8.4.json', date '19.11.2025', and author 'analyst@analyst.ru'. The report type is 'SBOM' and the status is 'Готово'. At the bottom, there is a code editor showing a snippet of JSON data representing the SBOM components.

```

13 components: [
14   {
15     "name": "389-ds-base",
16     "type": "application",
17     "version": "2.3.4+dfsg1-1.astra4",
18     "properties": [
19       {
20         "name": "GOST:attack_surface",
21         "value": "yes"
22       },
23       {
24         "name": "GOST:security_function",
25         "value": "indirect"
26       }
27     ],
28     "externalReferences": [
29       {
30         "url": "https://snapshot.debian.org/archive/debian/20230620T034349Z/pool/main/3/389-ds-base/389-ds-base_2.3.4+dfsg1.orig.tar.xz",
31         "type": "source-distribution",
32         "hashes": [
33           {
34             "alg": "STREEBOG-256",
35             "content": "7c7b4f74ec3e1dac7992579ad9f8af08994cb53f7d40fea361368bd25a01803a"
36           }
37         ]
38       }
39     ]
40   }
41 ]

```

Управление уязвимостями

Приоритизация

Трендовость

комплексная оценка критичности уязвимости по >10 показателям

Экосистемность

учет сценариев эксплуатации и поверхности атаки продуктов экосистемы

Непрерывность

постоянный контроль >30 источников информации

CVE-2025-68792 Трендовая

Пакет	Поверхность атаки
linux	Поверхность атаки (1.6_main, 1.7_main, 4.7_main, 8.1_main)
linux-5.10	Поверхность атаки (1.6_main, 1.7_main, 4.7_main, 8.1_main)
linux-5.15	Поверхность атаки (1.6_main, 1.7_main, 4.7_main)
linux-6.1	Поверхность атаки (1.7_main, 1.8_main, 3.8_main, 4.7_main)
linux-6.12	Поверхность атаки (1.8_main)
linux-6.6	Не лежит на поверхности атаки (без релиза)

Статус: Пред-черновой

Средний ipurkin

Паспорта | **Приоритизация** | УБИ | Архитектура и модель угроз | Трекер задач | Продукты ГК

Поиск по ВТ... + Добавить запись

ВТ | SEC

ВТ	CVE
ВТ-2323	ASE-9090-9090 CVE-2020-2020 Всего: 2
ВТ-91890	ASE-3030-3030 CVE-2025-0000 CVE-2026-1801 Всего: 3
ВТ-91887	CVE-2026-1801 Всего: 1
ВТ-91883	CVE-2026-1801 Всего: 1

Паспорта | Приоритизация | УБИ | Архитектура и модель угроз | Трекер задач | **Продукты ГК** |

Управление уязвимостями

Контроль и генерация артефактов

Автоматизированный контроль наличия патчей

Регрессионный анализ PoC

Методические рекомендации (MP) по нейтрализации угроз с учетом встроенных механизмов защиты

Отправка и постоянный контроль данных в БДУ ФСТЭК России

OVAL-описания с интегрированными MP

Непрерывное взаимодействие с VM-вендорами

PATCH CHECKER

- Главная страница
- Поиск CVE
- Аналитика
- Отчеты
- Пакеты и их зависимости
- Карточки CVE
- Эксплойты
- Документация
- Выход

CVE-2024-6232 Не трендовая CVE Статус: Проверено

There is a MEDIUM severity vulnerability affecting CPython. Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives.

Дата добавления в БД: 21.01.2026

Пакеты и их версии

python3.12	руру	python3.4	python3.11	python3.7	python2.7	python3.13	руру3	python3.9	python3.5
Уязвимо с:	Уязвимо с:	Уязвимо с:	Уязвимо с:	Уязвимо с:	Уязвимо с:	Уязвимо с:	Уязвимо с:	Уязвимо с:	Уязвимо с:
Исправлено в 3.12.6-1	Исправлено в	Исправлено в	Исправлено в	Исправлено в	Исправлено в	Исправлено в 3.13.0~rc2-1	Исправлено в 7.3.18+dfsg-1	Исправлено в	Исправлено в

CVE в обновлении

Версия	Ссылка на коммит	Статус	Действие
1.8.3.7	https://github.com/python/cpython/commit/ed3a49ea734ada357ff4442996fd4ae71d253373	Не актуально	Патч полностью применён
1.8.3.8	https://github.com/python/cpython/commit/4eaf4891c12589e3c7bdad5f5b076e4c8392dd06	Не актуально	Патч полностью применён
1.8.3.8	https://github.com/python/cpython/commit/743acbe872485dc18df4d8ab2dc7895187f062c4	Не актуально	Патч полностью применён
1.8.3.8	https://github.com/python/cpython/commit/d449caf8a179e3b954268b3a88eb9170be3c8fbf	Не актуально	Патч полностью применён
1.8.3.8	https://github.com/python/cpython/commit/ed3a49ea734ada357ff4442996fd4ae71d253373	Не актуально	Патч полностью применён
1.8.4.48	https://github.com/python/cpython/commit/4eaf4891c12589e3c7bdad5f5b076e4c8392dd06	Не актуально	Патч полностью применён

```

20 ...-07-02-13-39-20 gh-issue-121285 hrl-YI.zst | 2 +
21 3 files changed, 111 insertions(+), 38 deletions(-)
22 create mode 100644 Misc/NEWS.d/next/Security/2024-07-02-13-39-20 gh-issue-121285 hrl-YI.zst
23
24 diff --git a/Lib/tarfile.py b/Lib/tarfile.py
25 index 495349f08f9e76..3ab6811d63335b 100755
26 --- a/Lib/tarfile.py
27 +++ b/Lib/tarfile.py
28 @@ -841,6 +841,9 @@ def data_filter(member, dest_path):
29  # Sentinel for replace() defaults, meaning "don't change the attribute"
30  _KEEP = object()
31
32  ** Header length is digits followed by a space
33  + header_length_prefix_re = re.compile(br"([0-9]{1,20}) ")
34  +
35  class TarInfo(object):
  
```

Выявление нежелательного контента



>170 решенных задач



анализ сетевой активности



непрерывное взаимодействие с клиентами

Пропаганда

- × python3-cherryPy3
- × php-voku-portable-ascii
- × lua-busted
- × gitlab-1st
- × darktable
- × arangodb3
- × php-masterminds-html5
- × php-symfony-framework
- × и др.

Вредоносные ресурсы

- × foreman-assets
- × libonig-dev
- × libmng-dev
- × libimage-exiftool-perl
- × libxml-rss-perl
- × libccid
- × fiona-doc
- × texlive-latex-extra
- × и др.

18+ и онлайн казино

- × python3-wsaccel
- × python-txaio-doc
- × golang-github-go-
- × entry-go-license-
- × detector-dev
- × openocd
- × ruby-bacon
- × nmap-common
- × mariadb-test-data
- × и др.

Статический анализ

База данных доверия



Автоматизация рутинных задач, регулярность и балансировка нагрузки

Выставление критериев, сбор статистики и метрик



Интеграция с инструментами CI и трекером задач

Единые правила настройки инструментов анализа



Распределение задач между командами и профильными специалистами

Перенос и наследование разметки с различных сервисов

Срабатывания

Фильтры 7 | Мои пресеты | Нет применённых пресетов

Разметка от средств | Крит: 10 (10) 0 (0) 0 (0) 0 (0) 0 (0) | 23% 10 / 44

По ID | Колонки | Поиск по файлу, ID, багтрекеру, срабатыванию

Файл	Срабатывание	Инструменты	Статус (Эксперты)	Критичность (Эксперты)	Моя разметка
251806+astra11 Lib/encodings/__init__.py:111:0	SvEng.ND.6.DEREF_OF_NULL.EX After having been assigned to a None value at __init__.py:108, reference 'mod' is dereferenced at __init__.py:111.	Svace 40.250829	█	█	WON'T FIX UNCLEAR
251806+astra11 Tools/unicode/makeunicodedata.py:942:0	SvEng.ND.6.DEREF_OF_NULL.EX After having been assigned to a None value at makeunicodedata.py:933, reference 'field' is dereferenced at makeunicodedata.py:942.	Svace 40.250829	█	█	WON'T FIX UNCLEAR
indent.py:462, reference		Svace 40.250829	█	█	FALSE POSITIVE UNCLEAR
okenize.py:353, reference		Svace 40.250829	█	█	FALSE POSITIVE UNCLEAR
okenize.py:491, reference		Svace 40.250829	█	█	FALSE POSITIVE UNCLEAR
ixdiv.py:295, reference		Svace 40.250829	█	█	WON'T FIX UNCLEAR

Активность за 30 дней

< 1 2 3 4 5 > 10 / page

Статический анализ

Применение SentinelAI



Если вы устали от...

- огромного объема результатов SAST-инструментов
- высокого процента FP-срабатываний
- обработки однотипных ошибок

Покрытие разметкой

Размеченные против неразмеченных уникальных срабатываний



Размечено

45 158

7.32%

Неразмечен

571 756

92.68%

Качество анализа

25115

Проанализировано

24122

Со статусом Svacer

2597

Расхождений

10.8%

Уровень расхождений

Типы расхождений

Svacer: Won't fix, Sentinel: false_posit...

1463

Svacer: Won't fix, Sentinel: confirmed

558

Svacer: False Positive, Sentinel: confir...

314

Svacer: Confirmed, Sentinel: false_po...

196

46

Severity-аналитика



Major
24537

Critical
3860

Normal
7380

Minor
2077

Severity	Всего	Confirmed	FP	Won't Fix	Pending
Major	24537	1517	15199	850	6984
Normal	7380	466	3333	38	3543
Critical	3860	402	2089	9	1360
Minor	2077	182	1003	40	852

Статический анализ

Применение SentinelAI



- протестировано для C/C++, Python, Java, C#
- проверено на >700 проектах
- применимо для всех продуктов экосистемы
- позволило сэкономить уже более 2 ч/лет на разметке кода
- уже сейчас предлагает патчи для исправления

От ручного запуска до автоматизации и валидации на основе ML



353 д 13 ч

Сэкономленное время

106772ce-70e6-4f04-9958-73d05d04016b Завершено

[Открыть в SVACER](#)

/src/ausearch-avc.c

^ Скрыть исправление

Код исправления

```
// ... existing code ...

newnode = malloc(sizeof(anode));
if (newnode == NULL) {
    return;
}

// ... existing code ...
```



Динамический анализ

Платформа AutoFuzz



- автоматизация сборки и запуска оберток
- запуск вручную, по коммитам или по расписанию
- дедупликация крешей
- регрессионное тестирование
- интеграция с БДД

Платформа автоматизации фаззинг-тестирования



>350

проектов интегрировано в платформу фаззинг-тестирования

>10

версий и конфигураций ядер ОС подвергаются фаззинг-тестированию на платформах x86_64, arm64, s390x

>5000

фаззинг-оберток применяются для тестирования затрагиваемых ими изменений кода

>400

обнаруженных и устраненных проблем безопасности

>800

ядер CPU обеспечивают непрерывность процессов фаззинг-тестирования

3&3

три инструмента фаззинга (AFL++, libfuzzer, atheris) и три языка программирования (C/C++, python, go) поддерживаются на платформе

Динамический анализ

Фаззинг-тестирование



>80 выявленных и устраненных проблем безопасности

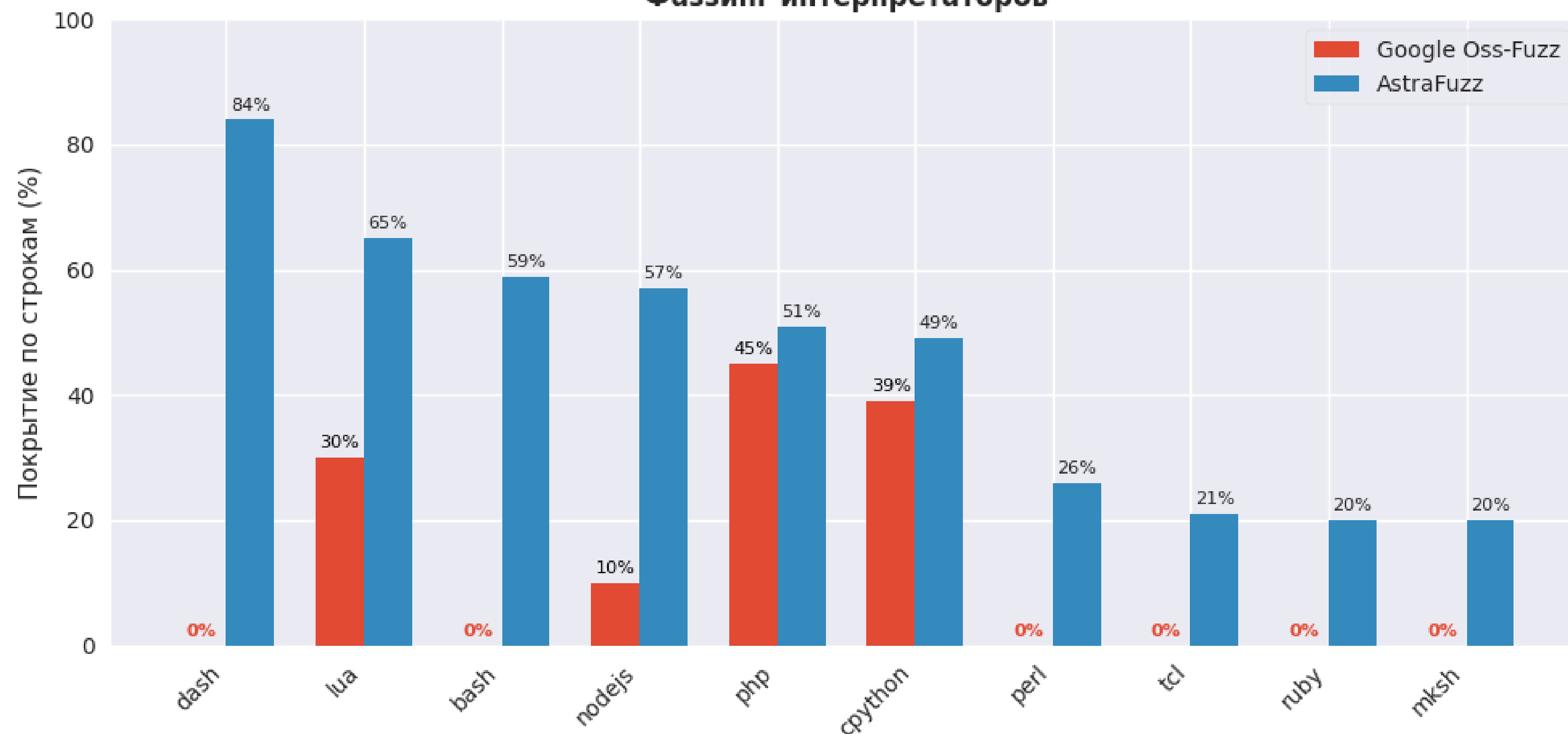


Непрерывное тестирование новых версий



Академический подход: эксперименты, методики, инструменты, сообщество

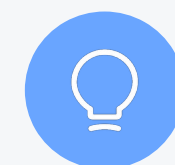
Фаззинг интерпретаторов



Модель угроз и поверхность атаки



- динамически меняется в ходе жизненного цикла ОС и продуктов экосистемы
- учитывается при развитии и разработке дополнительных механизмов безопасности продуктов экосистемы



Модель угроз

- включает более 160 актуальных УБИ
- оценивает каждую УБИ в отдельности и в рамках укрупненных групп
- постоянно актуализируется с учетом расширения сценариев применения
- формируется с учетом встроенных механизмов защиты



Детализация объектов воздействия

- ядро и модули ядра ОС
- средства защиты информации
- сетевые сервисы
- системное ПО
- графическая среда
- интерпретаторы
- прикладное ПО



Поверхность атаки

- детализируется с учетом уровня критичности последствий реализации УБИ:
 - высокий
 - средний
 - низкий
- пересматривается в ходе проведения анализа безопасности



Механизмы защиты ОС

- применимы для нейтрализации более 150 УБИ
- оцениваются по уровню эффективности
- развиваются для нейтрализации УБИ с учетом актуальной МУ
- составляют поверхность атаки

Основные инструментальные средства

Композиционный и статический анализ:

- Syft, Trivy, **ProtoPack**, **AVM**, **VulScan**
- Svace
- ClangSA
- AppScreener
- АК-BC 3
- CodeQL, semgrep, shellcheck
- **SentinelAI**

Динамический анализ:

- **Санитайзеры:** asan, lsan, kasan, ubsan, ...
- **Отладчики:** gdb, strace, ltrace, valgrind, uftrace
- **Сбор покрытия:** lcov, gcov, afl-cov
- **Фаззинг ядра:** syzkaller, **syz-ci**
- **Фаззинг:** crusher, afl++, libFuzzer, Sydr, go114-fuzz-build+go-fuzz-headers, **AutoFuzz**
- **А также:** klee, symcc, casr, ...

Средства верификации:

- Frama-C
- Verified Software Toolchain (VST)
- WP
- Why3
- Coq

А также:

- **Средства анализа ПА:** AttackSurfaceAnalyzer*, ...
- **Средства анализа помеченных данных:** «Блесна»
- **Средства тестирования на проникновение:** LinPEAS, Zap, Kali Linux*
- **Средства выявления нежелательного контента**
- **Средства антивирусного сканирования**
- ...

Программа «Bug Bounty»

BI.ZONE | BUG BOUNTY

Программы Только мои

« 🔍 ☰

- Активная Приватная Триаж BI.ZONE
 Rubackup
 не выплачивается 0 отчетов
- Активная Публичная Свой триаж
 DCImanager
 до 100 000 ₽ 12 отчетов > 5 дней
- Активная Публичная Триаж BI.ZONE
 ALD Pro
 до 100 000 ₽ 3 отчета
- Активная Публичная Триаж BI.ZONE
 ISPsystem: BILLmanager
 до 100 000 ₽ 24 отчета > 5 дней
- Активная Публичная Свой триаж
 Astra Linux SE 1.8.4
 до 250 000 ₽ 50 отчетов > 7 дней
- Активная Публичная Триаж BI.ZONE
 ISPsystem: VMmanager
 до 100 000 ₽ 23 отчета > 3 дней

Хакативность Программы Отчеты Войти

Активная Публичная Свой триаж
Astra Linux SE 1.8.4

Вознаграждение		Статистика Все время ▾	
Critical	0 - 0 ₽	2 395 000 ₽ всего выплат	108 863 ₽ средняя выплата
High	150 000 - 250 000 ₽	50 полученные отчеты	22 принятые отчеты
Medium	50 000 - 150 000 ₽		
Low	0 - 50 000 ₽		

Программа Задачи Топ исследователей Отчеты

Правила программы Markdown

Добро пожаловать в программу Bug Bounty Astra Linux Special Edition



СПАСИБО ЗА ВНИМАНИЕ

Тележников Владимир
Директор департамента
анализа безопасности, к.т.н.