

**Испытательная лаборатория
ООО Научно-технический центр «Фобос-НТ»**



Радости и горести современной сертификации

Борзов Роман
Кузнецов Андрей

Испытательная лаборатория ООО НТЦ «Фобос-НТ»

1

Система сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00.

Аттестат аккредитации испытательной лаборатории СЗИ RU.0001.01БИ00.Б039, выдан ФСТЭК России 20 марта 2020 г.

2

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (Система сертификации СЗИ-ГТ) РОСС RU.0003.01БИ00.

Аттестат аккредитации СЗИ RU.ЛИ0162, выдан ФСБ России 22 декабря 2020 г.

3

Система сертификации средств защиты информации по требованиям безопасности информации Министерства обороны Российской Федерации.

Аттестат аккредитации испытательной лаборатории № 401 от 06 июня 2022 г.



Горести

Управленческие

- Смотрите, у нас уже всё есть, когда будет сертификат?
- Продукт уже есть, давайте быстро сделаем документы!
- Нам нужен сертификат! Ресурсов очень мало, это не основное направление...
- Сделаем все на этой неделе, до пятницы точно скинем!
- Зачем собирать из исходников, что за требование? *Нормально же сидели...*

Инженерные

- У нас всё в контейнерах, это безопасно!
- Эти CVE не эксплуатируемы.
- Какие ещё интерпретаторы?!
- Что ещё за поверхность атаки?!
- Эти модули ни на что не влияют!

The screenshot shows a terminal window with the following output:

```
(root@kali) ~/home/user/cert_build_artifacts
trivy image ui
2022-11-09T19:11:29.223+0300 INFO Vulnerability scanning
2022-11-09T19:11:29.223+0300 INFO Secret scanning
2022-11-09T19:11:29.223+0300 INFO If your scan
d:\share\perl\5.28.1\*
```

Below the terminal, a file explorer window shows the directory structure:

- Имя
- [-]
- [App]
- [Archive]
- [Attribute]
- [au...]
- d:_webpu\share\gdb\auto-load\usr\lib\x86_64-linux-gnu\libstdc++.so.6.0.28-gdb.py
- d:_webpu\share\gcc\python\libstdc++\v6\printers.py
- d:_webpu\share\gcc\python\libstdc++\v6_init_.py
- d:_webpu\share\gcc\python\libstdc++_init_.py
- d:_webpu\python\libstdc++\v6\methods.py

At the bottom, a table displays vulnerability details:

Severity	Installed Version	Fixed Version	sqlite: Heap-buf
CRITICAL	3.9.2-r1	3.13.0-r1	https://avd.aqua



У нас всё в контейнерах, это безопасно!

```
{
  "id": "robotattack",
  "title": "Return Of Bleichenbacher's Oracle Threat",
  "desc": "ROBOT is the return of a 19-year-old vulnerability that allows perf
  "descriptions": [
    {
```

```
trivy image ui
2022-11-09T19:11:29.223+0300 INFO Vulnerability scanning is enabled
2022-11-09T19:11:29.223+0300 INFO Secret scanning is enabled
2022-11-09T19:11:29.223+0300 INFO If your scanning is slow, please try '--security-checks vuln' to disable secret scanning
2022-11-09T19:11:29.223+0300 INFO Please see also https://aquasecurity.github.io/trivy/v0.34/docs/secret/scanning/#recommendation for
2022-11-09T19:11:32.930+0300 INFO Detected OS: alpine
2022-11-09T19:11:32.930+0300 INFO Detecting Alpine vulnerabilities...
2022-11-09T19:11:32.934+0300 INFO Number of language-specific files: 0
2022-11-09T19:11:32.935+0300 WARN This OS version is no longer supported by the distribution: alpine 3.3.3
2022-11-09T19:11:32.935+0300 WARN The vulnerability detection may be insufficient because security updates are not provided

ui (alpine 3.3.3)
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 1)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version	Title
sqlite-libs	CVE-2017-10989	CRITICAL	3.9.2-r1	3.13.0-r1	sqlite: Heap-buffer overflow in the getNodeSize function https://avd.aquasec.com/nvd/cve-2017-10989



Эти CVE не эксплуатируемы

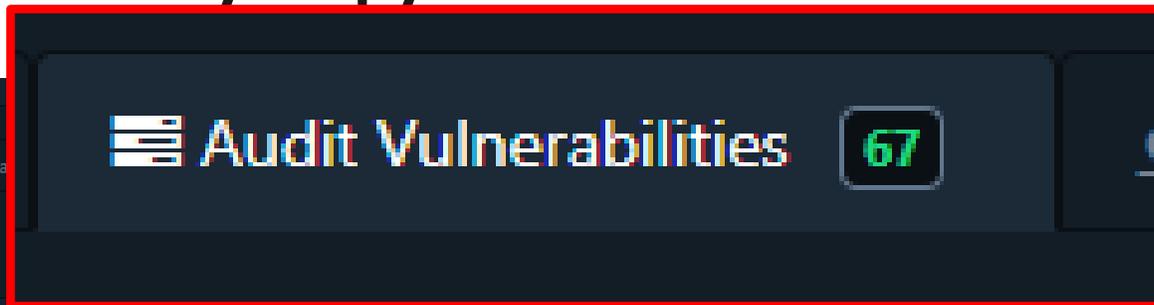
Details

Overview Components 300 Services 0 Dependency Graph 0 Audit Vulnerabilities 67 Policy Violations

Show suppressed findings

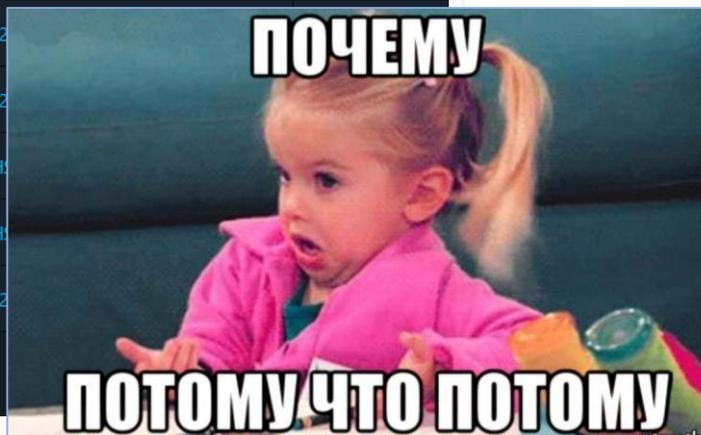
Component	Version	Group	Vulnerability	Severity
esapi	2.0.1	org.owasp.esapi	NVD CVE-2022-23457	Critical
solr-solrj	8.5.1	org.apache.solr	NVD CVE-2021-29943	Critical
spring-beans	5.2.7.RELEASE	org.springframework	NVD CVE-2022-22965	Critical
spring-boot-starter-web	2.3.1.RELEASE	org.springframework.boot	GITHUB GHSA-36p3-wjmg-h94x	Critical
spring-security-core	5.3.3.RELEASE	org.springframework.security	GITHUB GHSA-hh32-7344-cg2f	Critical
spring-web	5.2.7.RELEASE	org.springframework	NVD CVE-2022-22965	Critical
spring-web	5.3.21	org.springframework	NVD CVE-2022-22965	Critical
spring-webmvc	5.2.7.RELEASE	org.springframework	GITHUB GHSA-36p3-wjmg-h94x	Critical
tomcat-embed-core	9.0.36	org.apache.tomcat.embed	GITHUB GHSA-36p3-wjmg-h94x	Critical
itext	2.1.7	com.lowagie	NVD CVE-2022-22965	Critical

Showing 1 to 10 of 67 rows 10 rows per page



```
public sealed class JaegerHealthCheck : IHealthCheck
{
    private const string Description = "Проверка работоспос
    private const string HealthCheckName = "Jaeger";
    private readonly Lazy<HttpClient> _httpClient;
    private readonly IHttpClientFactory _clientFactory;

    private readonly IGaspsConfig _config;
```

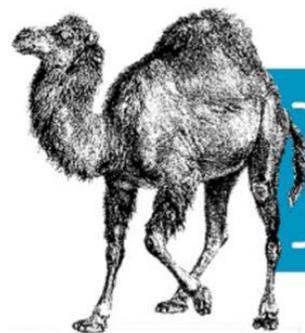
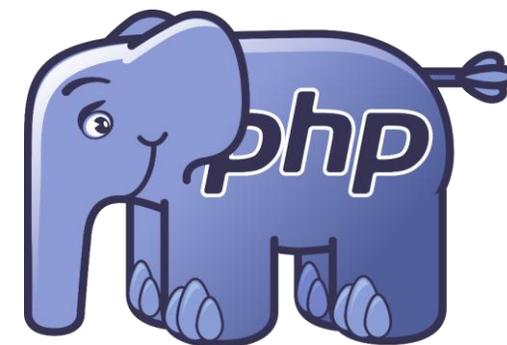


```
eritdoc cref="IHealthCheck.Id" />
tring Id { get; } = HealthCheckName;

eritdoc cref="IHealthCheck.DependencyType" />
ealthDependencyType DependencyType { get; } =
```



У нас нет интерпретаторов



Perl

Lua



The screenshot displays a static analysis tool interface. On the left, a sidebar lists files with associated issue counts. The main table shows findings with columns for Checker, File, Line, and Description. A specific finding for 'MEMORY_LEAK.EX' at line 1213 in 'ep.c' is highlighted. The right panel shows details for this issue, including a 'False Positive' status and a review by 's.tereshin'. A red box highlights the source code snippet for the issue, and a yellow circle highlights the file path in the table.

Checker	File	Line	Description
HIDDEN_MEMBER	Rectangle.cs	244	The struct member height of Rectangle is hidden by a para...
HIDDEN_MEMBER	Color.cs	488	The struct member value of Color is hidden by a local varia...
MEMORY_LEAK.EX	ep.c	1565	Dynamic memory referenced by 'exec_checkpoint' was allo...
MEMORY_LEAK.EX	ep.c	1213	Dynamic memory referenced by 'data_queue.queu...
MEMORY_LEAK.EX	ep-config.c	170	Dynamic memory referenced by 'callback_data_queue.que...
PROC_ADDR_NULL_CHECK	fx_muxer.cpp	112	Suspicious comparison with NULL of address of procedure ...
PROC_ADDR_NULL_CHECK	fx_muxer.cpp	173	Suspicious comparison with NULL of address of procedure ...
UNCHECKED_FUNC_RES.	pal.h	162	Return value 'return value of fputc(...) of a function 'fputw...
UNCHECKED_FUNC_RES.	pal.h	163	Return value 'return value of fputc(10__acrt_job_func(...))' ...
UNCHECKED_FUNC_RES.	pal.h	164	Return value 'return value of fputc(10__acrt_job_func(...))' ...
UNCHECKED_FUNC_RES.	pal.h	163	Return value 'return value of fputws(...) of a function 'fputw...
UNCHECKED_FUNC_RES.	ep.c	871	Return value 'return value of sprintf_s(...) of a function 'sprin...
UNCHECKED_FUNC_RES.	fx_muxer.cpp	458	Return value of a function 'pal:getenv' called at fx_muxer.c...
UNCHECKED_FUNC_RES.	deps_resolver.cpp	795	Return value of a function 'pal:realpath' called at deps_reso...
UNCHECKED_FUNC_RES.	deps_resolver.cpp	864	Return value of a function 'library_exists_in_dir' called at de...

```
Snapshot information Source code
/C_/a/b/d_00000000/s/dotnet/runtime/6.0.10/src/native/eventpipe/ep.c
1211 EventPipeProviderCall
1212 EventPipeProviderCall
False Positive Unspecified
allocated at ep.c:198 by call
a/b/d_00000000/s/dotnet/runtime/6.0.10/src/native/eventpipe/ep.c
1211 EventPipeProviderCallbackDataQueue data_queue;
1212 EventPipeProviderCallbackData provider_callback_data;
False Positive Unspecified Ignore MEMORY_LEAK.EX Dynamic memo
allocated at ep.c:198 by calling function 'ep_provider_callback_data_queue_init' at
EventPipeProviderCallbackDataQueue *provider_callback_data_queue = e
EP_LOCK_ENTER (section1)
provider = config_create_provider (ep_config_get (), provider_na
ep_raise_error_if_nok_holding_lock (provider != NULL, section1);
EP_LOCK_EXIT (section1)
while (ep_provider_callback_data_queue.try_dequeue (provider_callbac
```

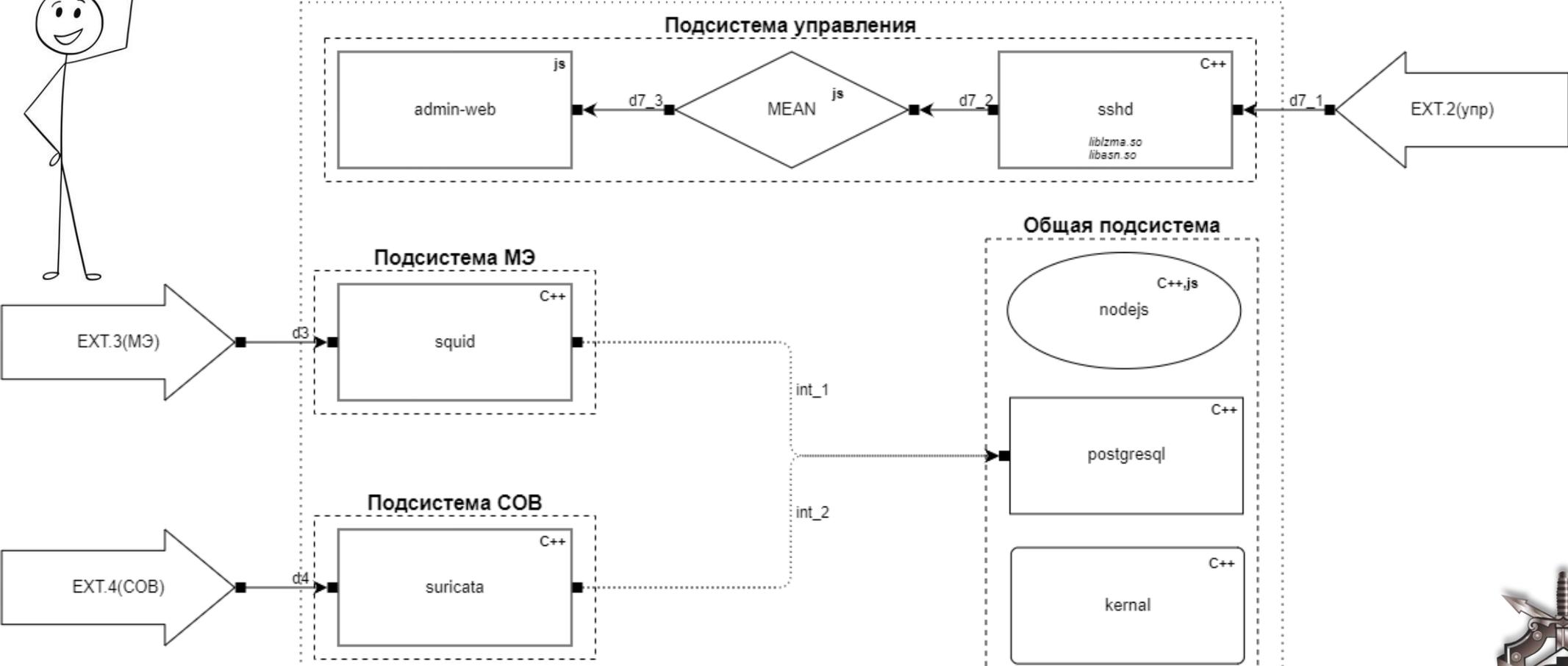
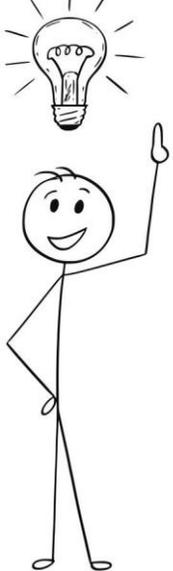


Определение поверхности атаки

- Не заявлены модули, реализующие функции безопасности.
- Заявлены модули, которые не обрабатывают данные.
- Ошибка определения большого количества ИФБО.
- Не включены модули, стоящие за другими, к которым нет прямого доступа.



Определение поверхности атаки



Практики безопасной разработки

- статический анализ;
- использование систем отслеживания известных уязвимостей;
- модульное и функциональное тестирование;
- фаззинг-тестирование;
- выявление побочных взаимодействий со средой функционирования;
- анализ утечек чувствительных данных;
- тестирование на проникновение.

**Автоматизация практик безопасной разработки (встраивание в CI/CD).
Обучение студентов и сотрудников в парадигме безопасной разработки.**



Инструмент для определения поверхности атаки Natch

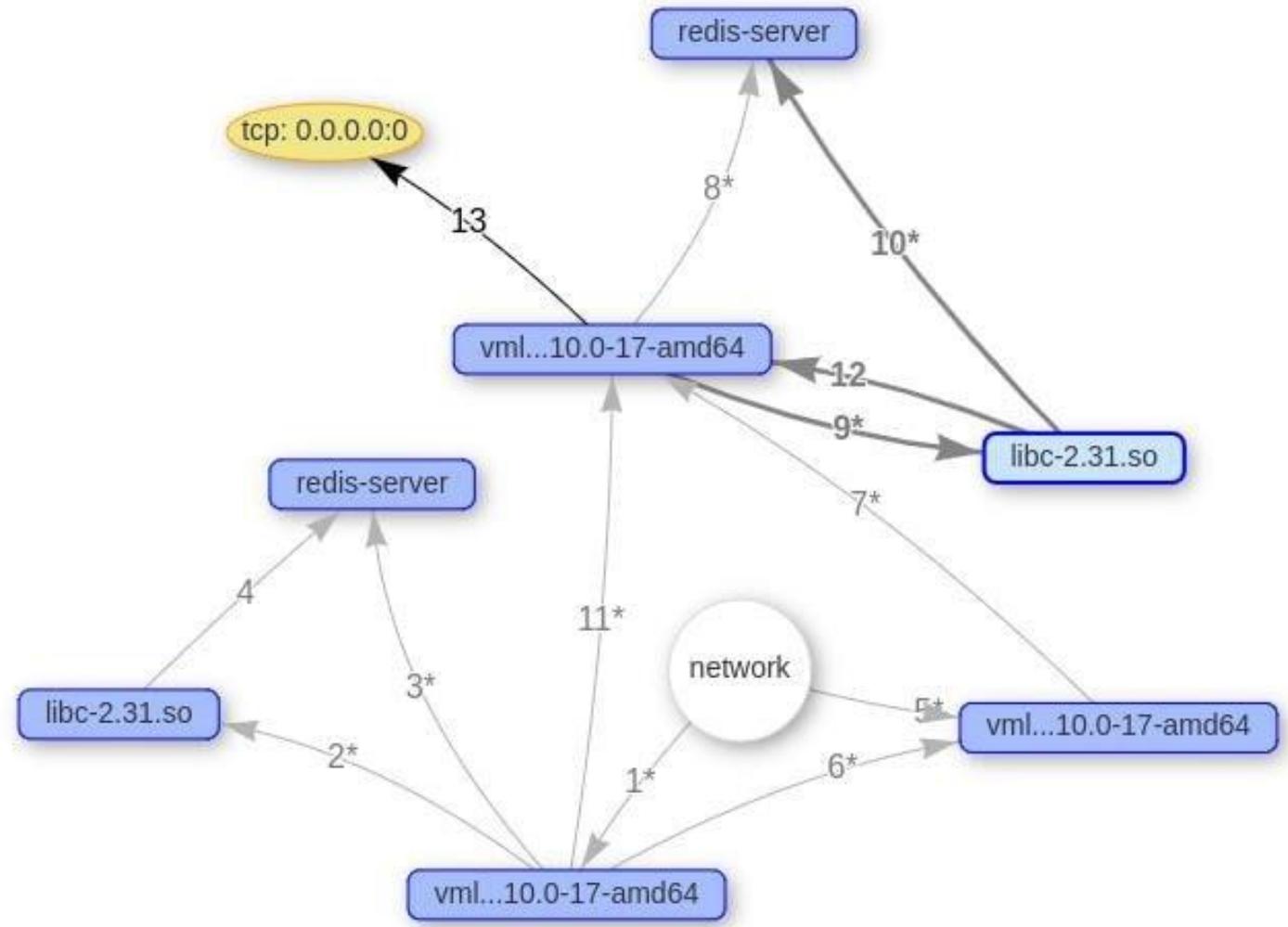


fNatch

[Upload an output.tar.zst](#)

- > Modules
- Additional graphs
 - Call-graph Ctrl+Alt+C
 - Flame-graph Generate
 - Process-graphs
 - Process-graph Ctrl+Alt+P
 - Process-graph content
 - Module-graph
 - Module-graph Ctrl+Alt+M
 - Module-graph content
 - Processes info
 - Process-timeline Ctrl+Alt+L
 - Process-tree Ctrl+Alt+R
 - Resources
- Settings
- About project

Projects -



Инструмент для определения поверхности атаки Natch



Upload an output.tar.zst

> Modules

Additional graphs

Call-graph Ctrl+Alt+C

Flame-graph

Process-graphs

Process-graph Ctrl+Alt+P

Process-graph content

Module-graph

python Call-graph x Process-gr

Options:

Hide symbolless graphs Full m

```

python
├─ 0x59548 (python)
│   └─ _libc_start_main (libc-2.31.so)
│       └─ main /home/user/cpython/Modules/main.c:30
│           └─ _Py_UnixMain /home/user/cpython/Modules/main.c:30
│               └─ pymain_main /home/user/cpython/Modules/main.c:30
│                   └─ pymain_run /home/user/cpython/Modules/main.c:30
│                       └─ pymain_run_file /home/user/cpython/Modules/main.c:30
└─ ...

```

```

#include <stdio.h>
#include <stddef.h>
#include <stdlib.h>
#include <string.h>
#include <stdint.h>
#include "curl_setup.h"
#include "warnless.h"

int LLVMFuzzerTestOneInput(uint8_t * Fuzz_Data, size_t Fuzz_Size){
    if (Fuzz_Size < sizeof(size_t)) return 0;
    uint8_t * pos = Fuzz_Data;
    //GEN_BUILTIN
    size_t uznum;
    memcpy(&uznum, pos, sizeof(size_t));
    pos += sizeof(size_t);
    //FUNCTION_CALL
    curlx_uztosz(uznum );
    //FREE
    return 0;
}

```



Блесна: инструмент динамического анализа помеченных данных

ИСП РАН

Поиск утечек

Автоматический режим

Список задач

Ручной режим

Трек

Вердикт

58392 - 8A9D3323] data v(0x6600AC8,...

Восстановить буфер Найти доступ

	0	1	2	3	4	5	6	7	8	9	A	B	C
0	53	00	45	00	43	00	52	00	45	00	54	00	50
10	53	00	53	00	00	00	AF						

Дерево вызовов Мод

Восстановить буфер

Поиск утечек

Автоматический режим

Список задач

Ручной режим

Трек

Вердикт

24156598 - 2FA83297] Data v(0...

24156674 - 2FA83297] Data v(0...

Восстановить буфер Найти доступ

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	01	23	45	67	89	AB	CD	EF								
E	user:	1234	@127.	0.												
0.1:	5000															

Восстановить буфер

Поиск утечек

Автоматический режим

Список задач

Ручной режим

Трек

Вердикт

0124B1ED3 - 1F5C33525] data v(0x250F6D0, 0x8)

0124B287B - 1F5C33525] data v(0x250F9C0, 0x8)

0124B3756 - 1F5C33525] data v(0x1010C68, 0x8)

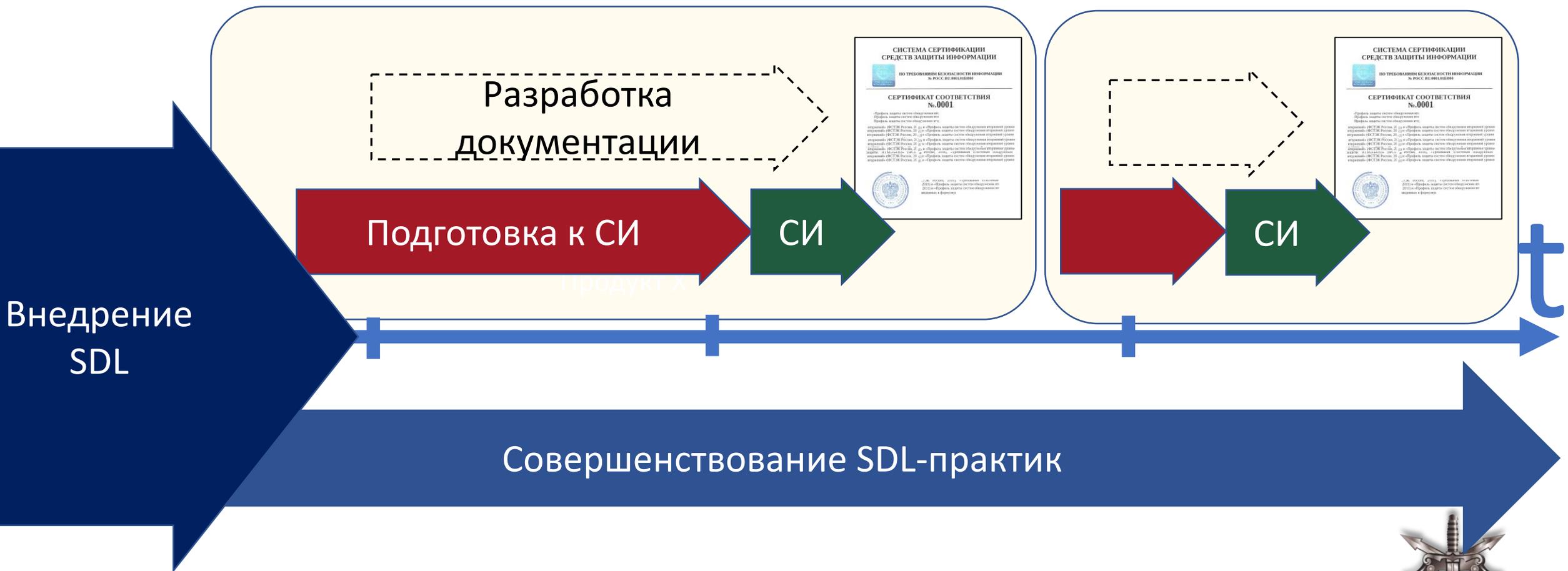
0124B3821 - 1F5C33525] data v(0x1010C98, 0x8)

Восстановить буфер Найти доступ

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	31	00	32	00	33	00	34	00								
																0123456789ABC
																1.2.3.4.

Восстановить буфер





Спасибо за внимание!

Борзов Роман Викторович, r.borzov@fobos-nt.ru

Кузнецов Андрей Викторович, a.kuznetcov@fobos-nt.ru

<https://fobos-nt.ru>

