Ideco ISG

Проектируем решение для защиты АСУ ТП

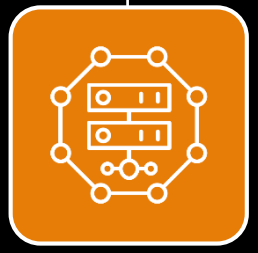
Руслан Никифоров

Заместитель директора по развитию

Айдеко – российский разработчик решений для сетевой безопасности

фильтрация трафика

защита сети



развитие сетевых инфраструктур

Защищаем сети компаний межсетевым экраном Ideco UTM

2005
мы стартовали на рынке ИБ

4 000
компаний используют Ideco UTM

40 000
человек используют VPN-подключения

2 000
бесплатных лицензий для некоммерческого использования

2020
начали сами работать удаленно

ideco

UTM/NGFW

Модули Ideco UTM:

DPI Фильтрация на 7 уровне модели OSI

15 млн доменов и IP-адресов C&C в нашем BlockList

500 млн URL в обновляемой базе данных

ideco

Соответствие требованиям регулятора

Сертификат ФСТЭК №4503
от 28.12.2021 г.

- Требования доверия (4)
- Требования к МЭ
- Требования к СОВ

Решение входит в реестр
российского ПО Минцифры РФ

- Профиль защиты МЭ (А четвертого класса защиты. ИТ.МЭ.А4.ПЗ)
- Профиль защиты МЭ (Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ)
- Профиль защиты СОВ (четвертого класса защиты. ИТ.СОВ.С4.ПЗ)

ideco

Customer success

Гибкая разработка

Моментальная реакция на новые вызовы и угрозы
Road-map по задачам пользователей

Защита сети «из коробки»

Преднастроенные правила фильтрации, IPS, FW

Шай-тек (Shy-tech)

Умные технологии для интуитивно понятных решений

Многоканальная техподдержка

-портал поддержки help.ideco.ru
-электронная почта
-телефон
-Telegram
-чат в продукте

Customer success

Выделенный менеджер для каждого
Фокус на долгосрочное партнерство
CustDev и проблемные интервью
Близко к community

Presale

Поддержка и консультации на этапе тестирования и внедрения
Решения для нестандартных кейсов

ideco

SDL

Документация

Проектная документация:
описание взаимосвязи моделей
в системе, пакетной базы

Поверхность атаки

Составление
поверхности атаки

Тестирование

Модульное

Анализ

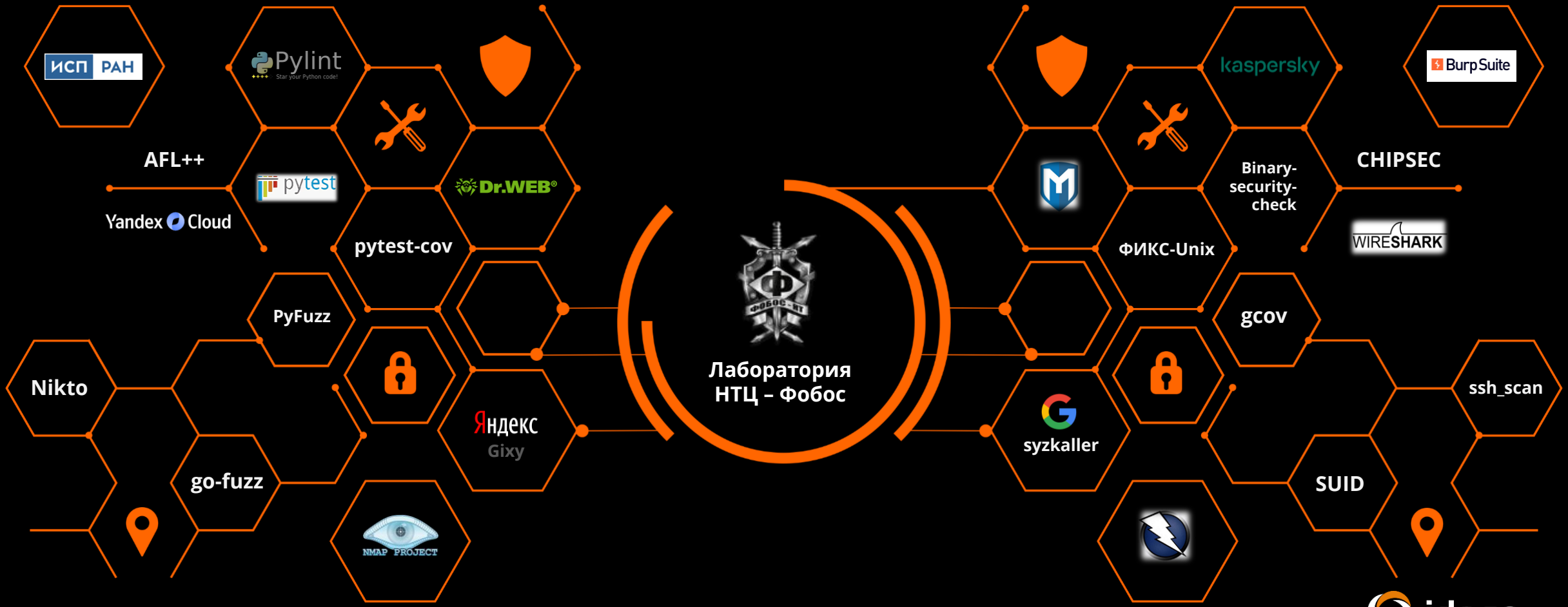
Статический
и динамический

Проверка

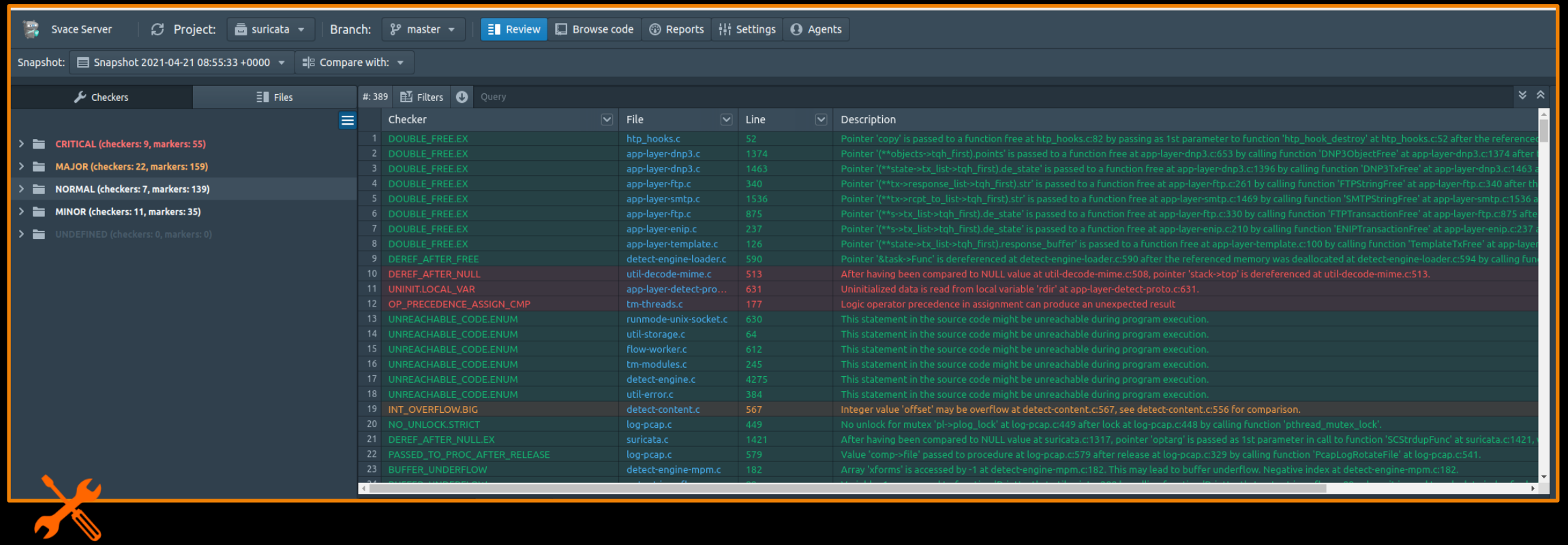
Лексемы
Различными сканерами безопасности
Автоматическая и ручная
по базе уязвимостей CVE

ideco

Инструменты безопасной разработки

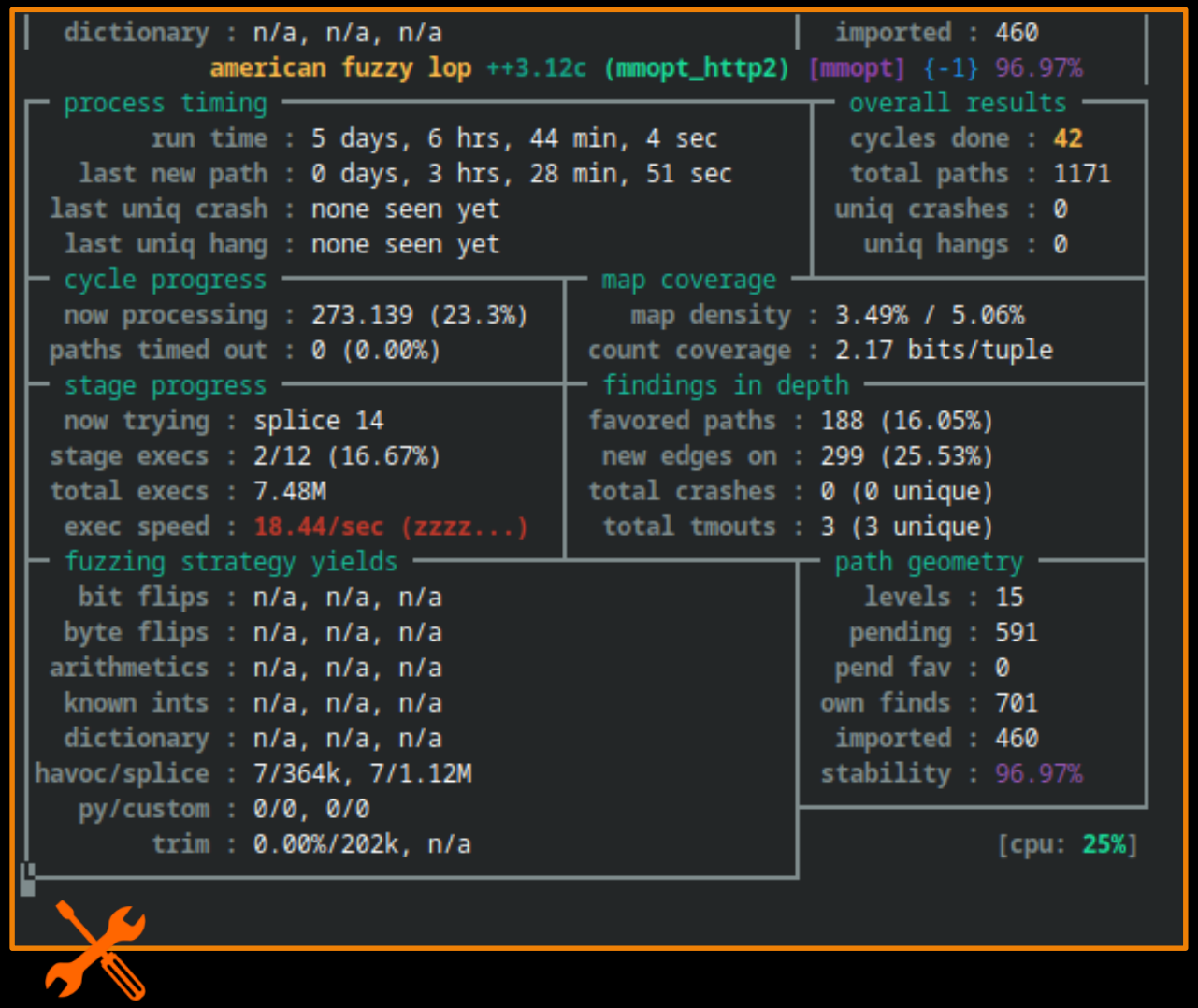


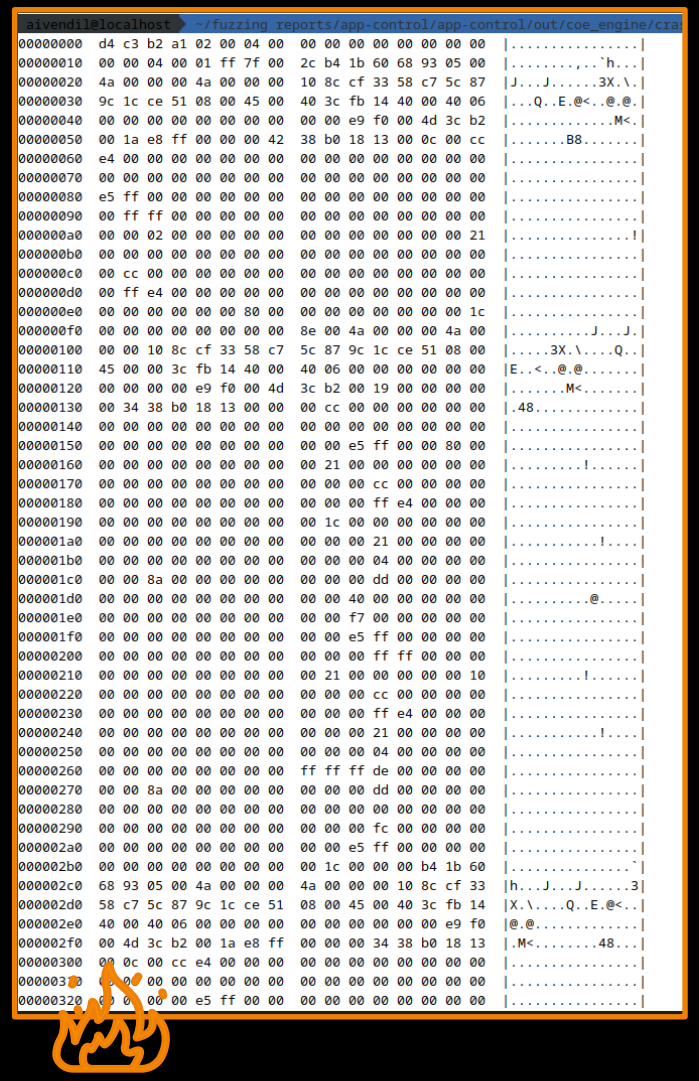
Svace


Svace Server
Project: suricata
Branch: master
Review
Browse code
Reports
Settings
Agents
Snapshot: Snapshot 2021-04-21 08:55:33 +0000
Compare with:
Checkers
Files
#: 389
Filters
Query
CRITICAL (checkers: 9, markers: 55)
MAJOR (checkers: 22, markers: 159)
NORMAL (checkers: 7, markers: 139)
MINOR (checkers: 11, markers: 35)
UNDEFINED (checkers: 0, markers: 0)
Checker
File
Line
Description
1 DOUBLE_FREE.EX htp_hooks.c 52 Pointer 'copy' is passed to a function free at htp_hooks.c:82 by passing as 1st parameter to function 'htp_hook_destroy' at htp_hooks.c:52 after the reference
2 DOUBLE_FREE.EX app-layer-dnp3.c 1374 Pointer '(**objects->tqh_first).points' is passed to a function free at app-layer-dnp3.c:653 by calling function 'DNP3ObjectFree' at app-layer-dnp3.c:1374 after
3 DOUBLE_FREE.EX app-layer-dnp3.c 1463 Pointer '(**state->tx_list->tqh_first).de_state' is passed to a function free at app-layer-dnp3.c:1396 by calling function 'DNP3TxFree' at app-layer-dnp3.c:1463
4 DOUBLE_FREE.EX app-layer-ftp.c 340 Pointer '(**tx->response_list->tqh_first).str' is passed to a function free at app-layer-ftp.c:261 by calling function 'FTPStringFree' at app-layer-ftp.c:340 after th
5 DOUBLE_FREE.EX app-layer-smtp.c 1536 Pointer '(**tx->rcpt_to_list->tqh_first).str' is passed to a function free at app-layer-smtp.c:1469 by calling function 'SMTPStringFree' at app-layer-smtp.c:1536
6 DOUBLE_FREE.EX app-layer-ftp.c 875 Pointer '(**s->tx_list->tqh_first).de_state' is passed to a function free at app-layer-ftp.c:330 by calling function 'FTPTransactionFree' at app-layer-ftp.c:875 afte
7 DOUBLE_FREE.EX app-layer-enip.c 237 Pointer '(**s->tx_list->tqh_first).de_state' is passed to a function free at app-layer-enip.c:210 by calling function 'ENIPTransactionFree' at app-layer-enip.c:237
8 DOUBLE_FREE.EX app-layer-template.c 126 Pointer '(**state->tx_list->tqh_first).response_buffer' is passed to a function free at app-layer-template.c:100 by calling function 'TemplateTxFree' at app-layer
9 DEREF_AFTER_FREE detect-engine-loader.c 590 Pointer '&task->Func' is dereferenced at detect-engine-loader.c:590 after the referenced memory was deallocated at detect-engine-loader.c:594 by calling fun
10 DEREF_AFTER_NULL util-decode-mime.c 513 After having been compared to NULL value at util-decode-mime.c:508, pointer 'stack->top' is dereferenced at util-decode-mime.c:513.
11 UNINIT.LOCAL_VAR app-layer-detect-pro... 631 Uninitialized data is read from local variable 'rdir' at app-layer-detect-proto.c:631.
12 OP_PRECEDENCE_ASSIGN_CMP tm-threads.c 177 Logic operator precedence in assignment can produce an unexpected result
13 UNREACHABLE_CODE.ENUM runmode-unix-socket.c 630 This statement in the source code might be unreachable during program execution.
14 UNREACHABLE_CODE.ENUM util-storage.c 64 This statement in the source code might be unreachable during program execution.
15 UNREACHABLE_CODE.ENUM flow-worker.c 612 This statement in the source code might be unreachable during program execution.
16 UNREACHABLE_CODE.ENUM tm-modules.c 245 This statement in the source code might be unreachable during program execution.
17 UNREACHABLE_CODE.ENUM detect-engine.c 4275 This statement in the source code might be unreachable during program execution.
18 UNREACHABLE_CODE.ENUM util-error.c 384 This statement in the source code might be unreachable during program execution.
19 INT_OVERFLOW.BIG detect-content.c 567 Integer value 'offset' may be overflow at detect-content.c:567, see detect-content.c:556 for comparison.
20 NO_UNLOCK.STRICT log-pcap.c 449 No unlock for mutex 'pl->plog_lock' at log-pcap.c:449 after lock at log-pcap.c:448 by calling function 'pthread_mutex_lock'.
21 DEREF_AFTER_NULL.EX suricata.c 1421 After having been compared to NULL value at suricata.c:1317, pointer 'optarg' is passed as 1st parameter in call to function 'SCStrdupFunc' at suricata.c:1421,
22 PASSED_TO_PROC_AFTER_RELEASE log-pcap.c 579 Value 'comp->file' passed to procedure at log-pcap.c:579 after release at log-pcap.c:329 by calling function 'PcapLogRotateFile' at log-pcap.c:541.
23 BUFFER_UNDERFLOW detect-engine-mpm.c 182 Array 'xforms' is accessed by -1 at detect-engine-mpm.c:182. This may lead to buffer underflow. Negative index at detect-engine-mpm.c:182.

ideco

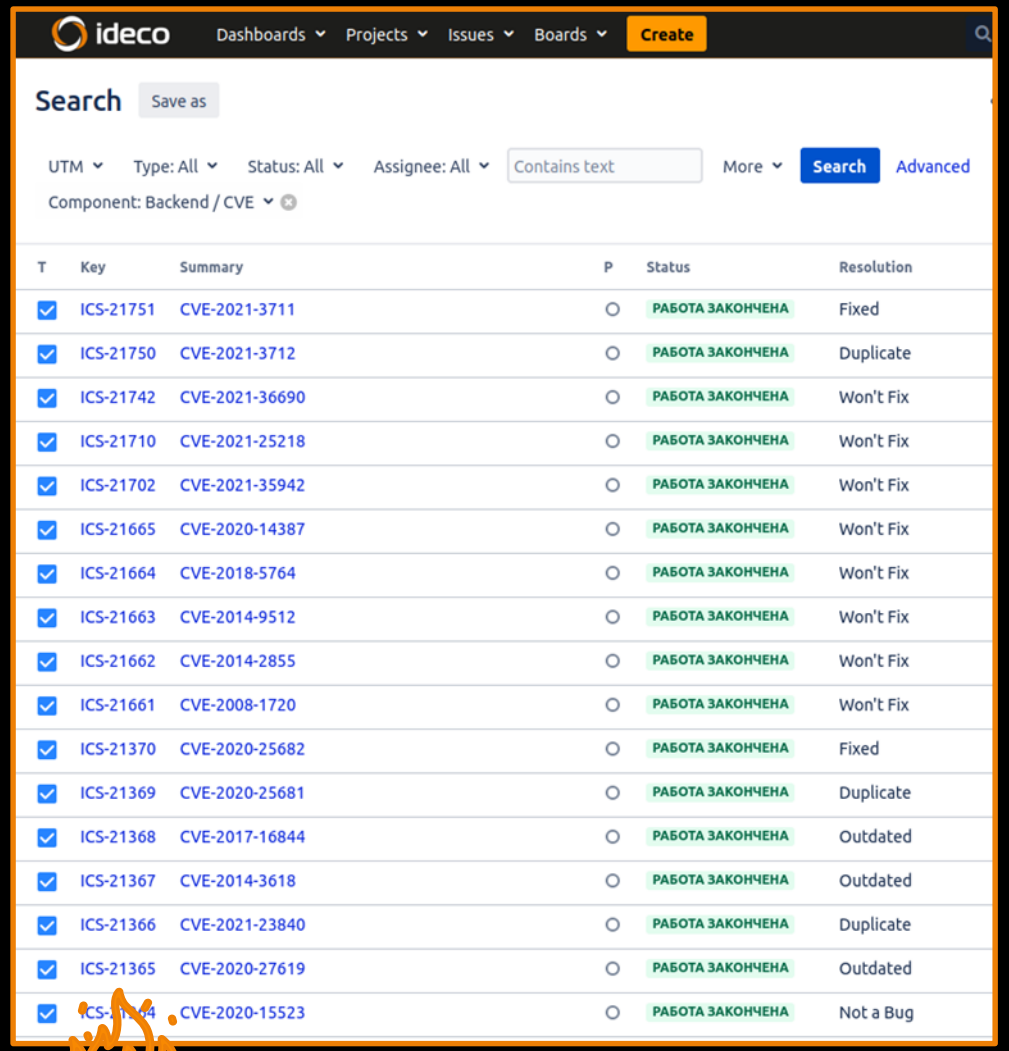
Фаззинг





ideco

CVE. Уязвимости



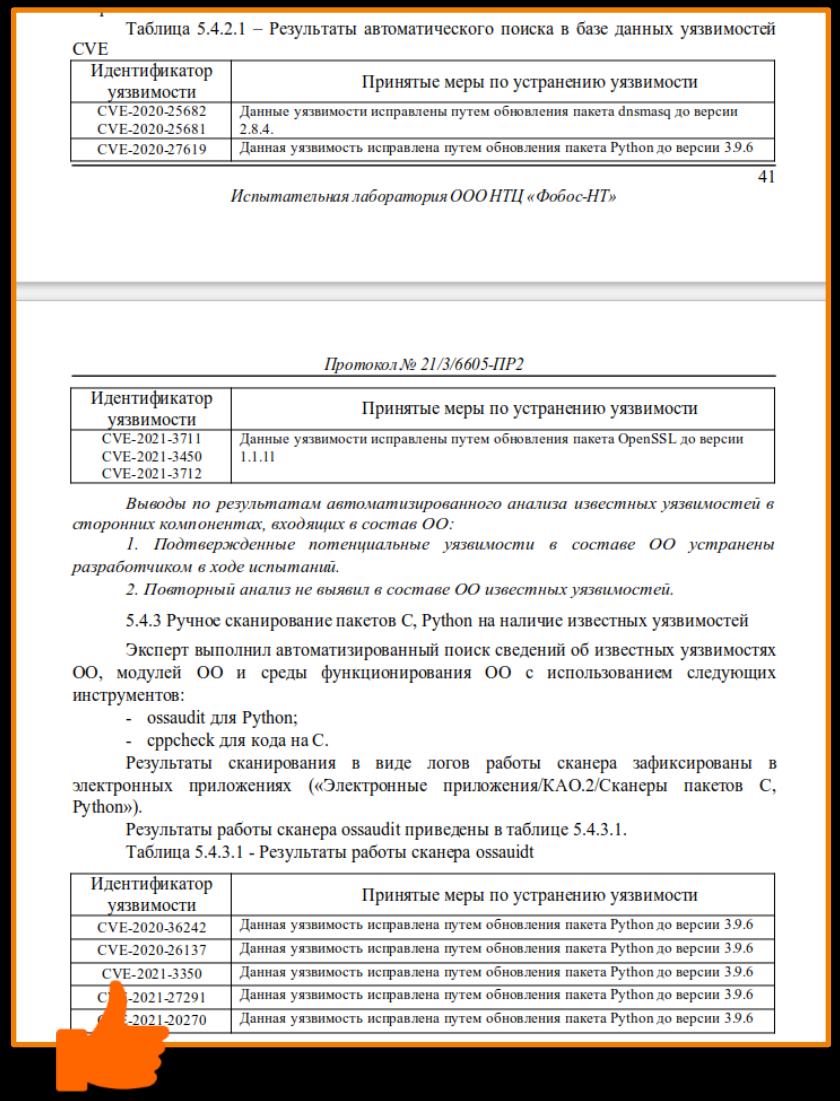


Таблица 5.4.2.1 – Результаты автоматического поиска в базе данных уязвимостей CVE

Идентификатор уязвимости	Принятые меры по устранению уязвимости
CVE-2020-25682 CVE-2020-25681	Данные уязвимости исправлены путем обновления пакета dnsmasq до версии 2.8.4.
CVE-2020-27619	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6

41

Испытательная лаборатория ООО НТЦ «Фобос-НТ»

Протокол № 21/3/6605-ПР2

Идентификатор уязвимости	Принятые меры по устранению уязвимости
CVE-2021-3711 CVE-2021-3450 CVE-2021-3712	Данные уязвимости исправлены путем обновления пакета OpenSSL до версии 1.1.1l

Выводы по результатам автоматизированного анализа известных уязвимостей в сторонних компонентах, входящих в состав ОО:

1. Подтвержденные потенциальные уязвимости в составе ОО устранены разработчиком в ходе испытаний.

2. Повторный анализ не выявил в составе ОО известных уязвимостей.

5.4.3 Ручное сканирование пакетов C, Python на наличие известных уязвимостей

Эксперт выполнил автоматизированный поиск сведений об известных уязвимостях ОО, модулей ОО и среды функционирования ОО с использованием следующих инструментов:

- ossaudit для Python;
- cppcheck для кода на C.

Результаты сканирования в виде логов работы сканера зафиксированы в электронных приложениях («Электронные приложения/КАО.2/Сканеры пакетов C, Python»).

Результаты работы сканера ossaudit приведены в таблице 5.4.3.1.

Таблица 5.4.3.1 - Результаты работы сканера ossauidt

Идентификатор уязвимости	Принятые меры по устранению уязвимости
CVE-2020-36242	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6
CVE-2020-26137	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6
CVE-2021-3350	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6
CVE-2021-27291	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6
CVE-2021-20270	Данная уязвимость исправлена путем обновления пакета Python до версии 3.9.6

ideco

Баг-трекер

ICS-20761 [svace] squid: src/acl/Random.cc:76: PROC_USE.VULNERABLE.SSCANF	ОЖИДАЕТ П...
ICS-20762 [svace] squid: src/auth/basic/RADIUS/basic_radius_auth.cc:592: UNREACHABLE_CODE.RET	ОЖИДАЕТ П...
ICS-20763 [svace] squid: src/ipc/mem/Pages.cc:67,76: OVERFLOW_UNDER_CHECK	ОЖИДАЕТ П...
ICS-20764 [svace] squid: src/ip/QosConfig.cc:322: SIMILAR_BRANCHES	ОЖИДАЕТ П...
ICS-20766 [svace] squid: lib/snmplib/parse.c:787: UNCHECKED_FUNC_RES.STAT	ОЖИДАЕТ П...
ICS-20767 [svace] squid: libltdl/ltdl.c:776: UNCHECKED_FUNC_RES.STAT	ОЖИДАЕТ П...
ICS-20768 [svace] squid: src/neighbors.cc:789: DEREF_OF_NULL.EX	ОЖИДАЕТ П...
ICS-20769 [svace] squid: NO_CAST.INTEGER_OVERFLOW: The value of an arithmetic expression 2*skew is subject to overflow	ОЖИДАЕТ П...
ICS-20770 [svace] squid: src/cf_gen.cc:381,390: NO_EFFECT	ОЖИДАЕТ П...
ICS-20771 [svace] squid: src/clients/FtpClient.cc:164: UNINIT.CTOR	ОЖИДАЕТ П...
ICS-20772 [svace] squid: src/auth/negotiate/kerberos/negotiate_kerberos_pac.cc:124,136: WRONG_ARGUMENTS_ORDER	ОЖИДАЕТ П...
~~ICS-20707~~ [svace] squid: lib/rfcnb/rfcnb-io.c:402: DEREF_AFTER_NULL.EX	РАБОТА ЗАКО...
~~ICS-20709~~ [svace] squid: src/ssl/support.cc:72: DEREF_OF_NULL.RET.LIB.PROC	РАБОТА ЗАКО...
~~ICS-20715~~ [svace] squid: src/urn.cc:388: MEMORY_LEAK	РАБОТА ЗАКО...
~~ICS-20751~~ [svace] squid: src/ssl/ErrorDetailManager.cc:212: BUFFER_OVERFLOW.EX	РАБОТА ЗАКО...
~~ICS-20754~~ [svace] squid: src/peer_digest.cc:728: NULL_AFTER_DEREF	РАБОТА ЗАКО...
~~ICS-20755~~ [svace] squid: src/store.cc:1463: NULL_AFTER_DEREF	РАБОТА ЗАКО...
~~ICS-20756~~ [svace] squid: src/store/Controller.cc:210: NULL_AFTER_DEREF	РАБОТА ЗАКО...
~~ICS-20757~~ [svace] squid: src/store_client.cc:316: NULL_AFTER_DEREF	РАБОТА ЗАКО...
~~ICS-20758~~ [svace] squid: tools/cachemgr.cc:819: DEREF_OF_NULL.RET.STAT	РАБОТА ЗАКО...
~~ICS-20759~~ [svace] squid: src/http.cc:1809: DEREF_OF_NULL.RET.STAT	РАБОТА ЗАКО...
~~ICS-20765~~ [svace] squid: src/anyp/Uri.cc:705: SIMILAR_BRANCHES	РАБОТА ЗАКО...

ideco

Ideco Industrial Security Gateway (Ideco ISG)

Инспекция АСУ-ТП протоколов:
IEC-61850 MMS, IEC-61850 GOOSE,
IEC-60870-5-104, МЭК-104,
MODBUS (TCP), S7-COM, OPC UA

Firewall

Оффлайн обновления
системы, сигнатур.
Работа шлюза без связи
с сервером лицензирования

Конфигурирование через JSON,
без веб-интерфейса

Сбор событий безопасности и
отправка их во внешние
системы (clickhouse? syslog?)

Кластеризация

Потоковый антивирус
SMB, FTP, SSH, HTTP

Реализация
сетевых интерфейсов без
разделения LAN/WAN

Резервирование
каналов

VPN (OpenVPN)

Работа с протоколом OPCDA
на базе DCERPC

ideco

ideco

Спасибо!

@RuslanNikiforov

r.nikiforov@ideco.ru

t.me/idecoutm

@ideco