Жизнь «Айдеко» в парадигме SDL

Андрей Орлов
Руководитель отдела сертификации

КОМПАНИЯ «IDECO»

Помогаем компаниям защитить сеть от современных угроз безопасности удобным и «умным» межсетевым экраном нового поколения Ideco NGFW. Экономим ваше время на настройке интернет-шлюза.

Используем собственные ноу-хау и базы данных, которые создаются с помощью технологий машинного обучения и искусственного интеллекта.

Ваша сеть – ваши правила с Ideco NGFW.

2023 Ideco VPP фильтрация трафика до 40 Гбит/сек. (4 квартал)
Ideco NGFW 16

2022 Ideco UTM 13 – с новой системой отчётов по трафику и IPS

2021 Ideco UTM 11: кластеризация и новейшие модули.
Сертификация ФСТЭК МЭ А4/Б4 и СОВ от 28 декабря 2021 г.

2020 Мгновенные ответы от технической поддержки в веб-интерфейсе.
Ideco UTM 8 на новейшей платформе (ядро Linux 5.9)

2016 Ideco UTM одним из первых вошел в «Единый реестр российских программ для ЭВМ и БД»

2015 Ideco ICS 6 получил сертификат ФСТЭК МЭ3/НДВ4

2011 SkyDNS, разработчик облачной системы DNS-фильтрации, выделен в отдельную компанию

2005 Релиз Ideco ICS – биллинговой системы для компаний и провайдеров.
Первый клиент – технический университет УГТУ (УПИ)

Более 5 000 компаний защищает Ideco NGFW

Наше решение блокирует 25 000 атак ежедневно

17 лет и 400 000 часов разработки

ВКЛАД В БЕЗОПАСНУЮ РАЗРАБОТКУ

09 февраля 2023 – m08

	Назначено	В работе	Подтверждено						Won't Fixed				False Positive			
			На оценке	В работе	Сообщено	Исправлено	в 5.10	Всего	Без вериф.	Обсуждается	Подтверждено	Всего	Без вериф.	Обсуждается	Подтверждено	Всего
01-bellsoft	**600**	184	11	10	-	24	4	**49**	122	14	79	**215**	48	-	104	**152**
02-basealt	**500**	11	-	67	1	4	3	**75**	85	22	279	**386**	8	1	19	**28**
03-astralinux	**510**	11	-	35	13	20	10	**78**	117	-	162	**279**	45	1	96	**142**
04-rosa	**550**	86	-	51	6	3	-	**60**	142	4	125	**271**	33	7	93	**133**
05-ivk	**500**	5	2	42	5	8	2	**59**	123	3	158	**284**	53	1	98	**152**
06-redsoft	**550**	36	-	73	3	9	2	**87**	111	1	150	**262**	60	1	104	**165**
07-yandex	**580**	72	1	34	8	11	4	**58**	115	-	143	**258**	81	-	111	**192**
08-aladdin	**500**	20	-	65	2	11	3	**81**	143	1	125	**269**	19	2	109	**130**
09-mcst	**550**	57	-	41	18	35	-	**94**	119	2	209	**330**	15	1	53	**69**
10-omp	**500**	15	1	47	-	36	3	**87**	115	3	145	**263**	55	5	75	**135**
12-securitycode	**550**	111	-	70	5	19	1	**95**	102	5	105	**212**	43	-	89	**132**
13-infotecs	**500**	1	-	21	-	16	14	**51**	131	-	153	**284**	45	-	119	**164**
14-swemel	**500**	3	-	8	8	6	1	**23**	189	11	205	**405**	7	-	62	**69**
15-fintech	**540**	-	-	-	7	28	33	**68**	138	1	237	**376**	17	1	78	**96**
16-factor-ts	**270**	72	-	9	10	3	1	**23**	24	-	89	**113**	9	-	53	**62**
17-confident	**500**	38	7	26	-	-	1	**34**	144	1	93	**238**	134	1	55	**190**
18-rasu	**570**	98	-	38	-	3	4	**45**	143	5	182	**330**	31	1	65	**97**
19-itb	**500**	103	2	104	-	-	-	**106**	58	8	47	**113**	83	2	93	**178**
20-ideco	**500**	97	-	71	-	2	1	**74**	124	9	149	**282**	11	-	36	**47**
21-nppct	**550**	10	16	17	-	1	-	**34**	175	3	224	**402**	26	-	78	**104**
22-usergate	**500**	13	4	45	-	2	-	**51**	268	-	159	**427**	3	-	6	**9**
23-vniief	**500**	163	-	1	-	-	-	**1**	122	1	173	**296**	30	-	10	**40**
24-msvsphere	**500**	117	-	105	-	5	-	**110**	83	-	49	**132**	89	-	52	**141**
25-ancud	**450**	203	5	3	6	20	-	**34**	23	4	88	**115**	5	1	92	**98**
26-t-argos	**40**	19	-	13	-	-	-	**13**	4	-	-	**4**	4	-	-	**4**
Всего:	**11820**	1323	44	980	86	246	87	**1443**	2893	94	3440	**6427**	945	24	1658	**2627**

SECURITY DEVELOPMENT LIFECYCLE

Автоматизировано:

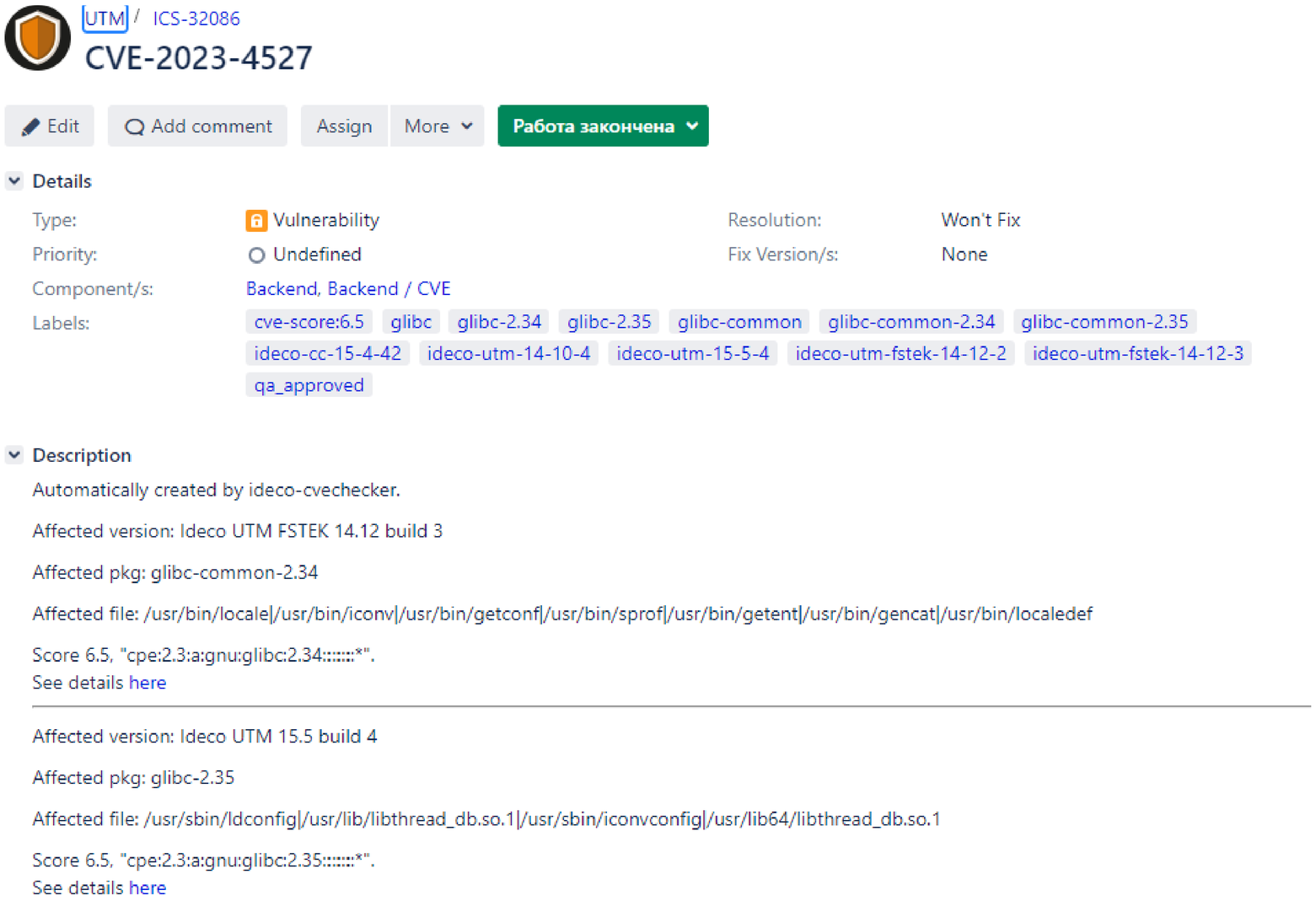
1. Пересборка всего
2. Поиск CVE и создание задач в Jira
3. Unit, интеграционные и нагрузочные тесты
4. Запуск линтеров
5. Запуск статического анализа Svace’ом
6. Анализ cppchecker’ом и ossaudit’ом
7. Фаззинг (AFL++, Syzkaller, Go-Fuzz)

Вручную:

Анализ прав доступа, поиск подозрительных лексем, binary-security-check, gixy, metasploit, nikto, nmap, OWASP ZAP, BurpSuite, ssh_scan, сбор трафика Wireshark’ом и др.

Что еще:

1. Уменьшение компонентной базы
2. Поиск НДВ
3. Обновление ПО
4. Борьба с supply chain attack
5. Architecure review
6. Code review
7. Runtime ограничение для всех процессов



НЕМНОГО ЦИФР

ideco

CVE-уязвимости

Найдено и исправлено - **227**

Статический анализ

Найдено - **301**
В апстрим отправлено - **13**

Фаззинг

Найдено - **49**
В апстрим отправлено - **11**

Объём

Исходников - **11,1 Гб**
Файлов - **522 тыс.**

К ЧЕМУ МЫ ПРИШЛИ

- Регулярное обновление используемых open source библиотек
- Регулярная проверка библиотек по открытым базам данных (bdu.fstek.ru, cve.mitre.org)
- Регулярная проверка кода статическими анализаторами
- Статический анализ не может найти все проблемы в коде
- Для выполнения всех проверок достаточно небольшой команды специалистов

СЕРТИФИКАЦИЯ И БЕЗОПАСНАЯ РАЗРАБОТКА

Приказ ФСТЭК России № 76 «Об утверждении требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»

Приказ ФСТЭК России № 121 "О внесении изменений в Положение о системе сертификации средств защиты информации, утвержденное приказом Федеральной службы по техническому и экспортному контролю от 3 апреля 2018 г. N 55"

БАЛАНС

ideco

КАЧЕСТВО ПРОДУКТА

СКОРОСТЬ ВЫПУСКА НОВЫХ РЕЛИЗОВ

ideco

СПАСИБО ЗА ВНИМАНИЕ

Андрей Орлов

Руководитель отдела сертификации

@Andrew0r

a.orlov@ideco.ru