Конференция ITSEC 09.10.2024

Актуальные вопросы управления уязвимостями в условиях импортозамещения

Наталья Онищенко, эксперт по ИБ

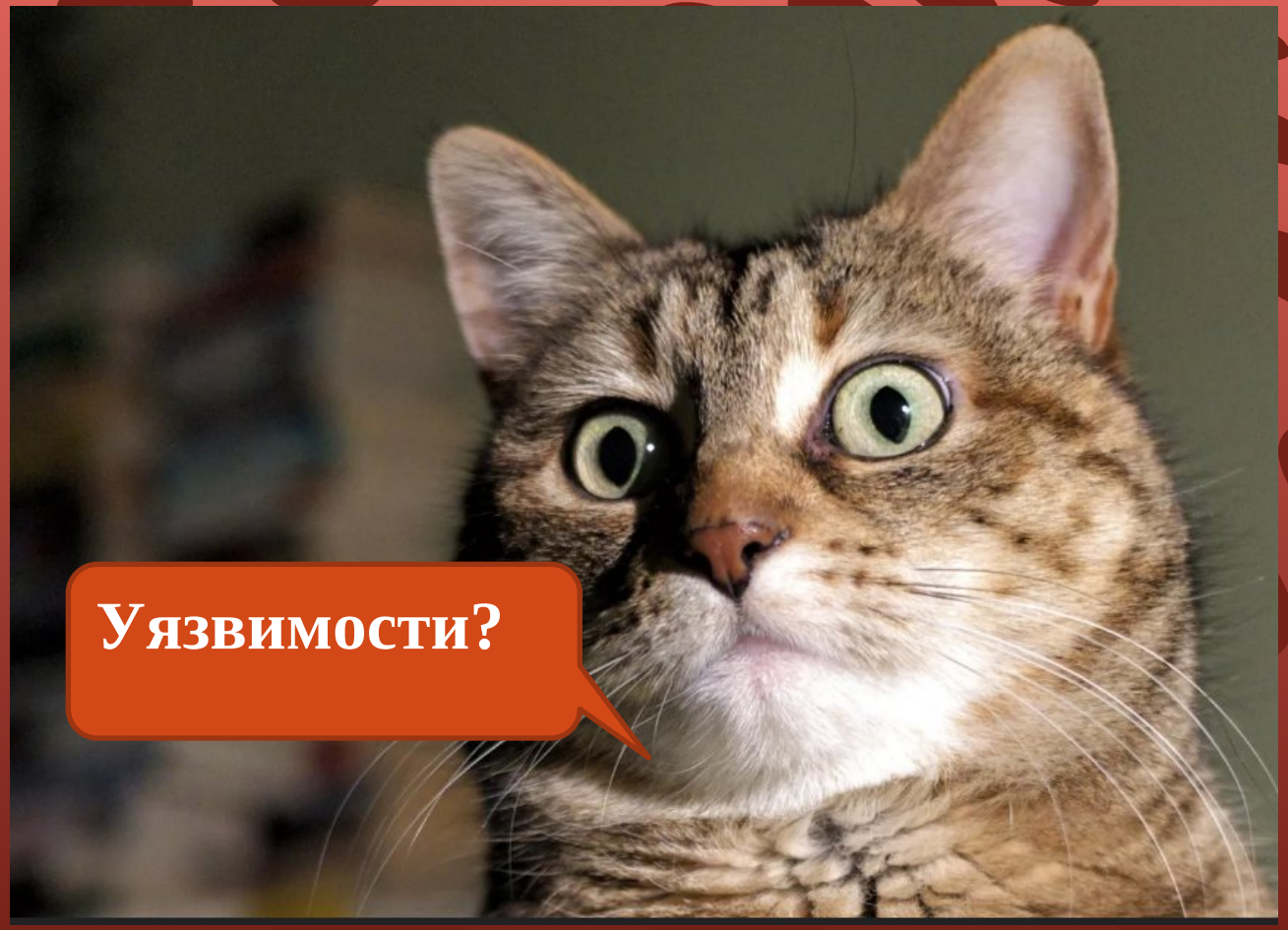

И наличие эксплойта подтвердил, прикинь
И обновление выложил час назад
Наташ, там наш вендор уязвимость опубликовал. Свежую!
Харош спать, го патчить уже!

Заказчик	Вендор
Все должно работать – мы за это платим	Безопасная разработка - это дорого
Новая прошивка – фичи добавились, глюки тоже	Новые фичи монетизируются лучше всего
Если не используются опенсорсные библиотеки, почему сканер показывает CVE? Часто, не самые свежие	Мы не используем опенсорсные библиотеки, поэтому не подвержены CVE
Нам важно понимать, каким уязвимостям подвержено ПО оборудования	Публикация уязвимостей – репутационные, считай, финансовые потери

Дихотомия потребностей

CVE ID	CVSS	EXPLOIT	PATCH
CVE-2024-9043 Secure Email Gateway from Cellopoint has Buffer Overflow Vulnerability in authentication process. Remote unauthenticated attackers...	CVSS 9.8	Exploit	-
CVE-2024-8188 The CVE description is not yet available but Feedly AI found some discussions about it	CVSS MEDIUM	-	-
CVE-2024-6744 The SMTP Listener of Secure Email Gateway from Cellopoint does not properly validate user input, leading to a Buffer Overflow...	CVSS 9.8	-	-
CVE-2024-47290 Input validation vulnerability in the USB service module Impact: Successful exploitation of this vulnerability may affect...	CVSS 5.5	-	Patched
CVE-2024-45163 The Mirai botnet through 2024-08-19 mishandles simultaneous TCP connections to the CNC (command and control) server....	CVSS 9.1	-	-

- Уязвимости Cisco за 2024г



- Уязвимости типового отечественного вендора за 2024 г

Хакеры не смогут использовать уязвимости, если они не знают о них

К. Очевидность: «На самом деле нет»

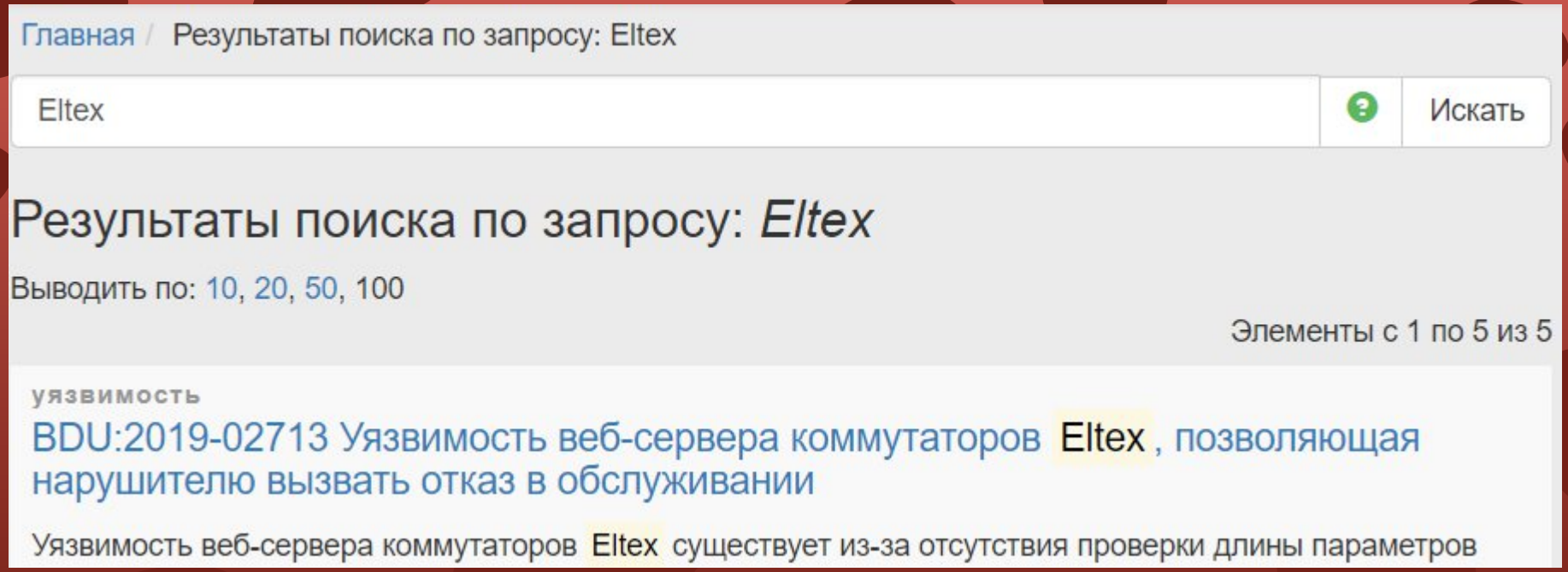
Повторить то, что делали Palo Alto или Checkpoint можно будет не раньше, чем через пять лет

(Рустэм Хайретдинов, Гарда)

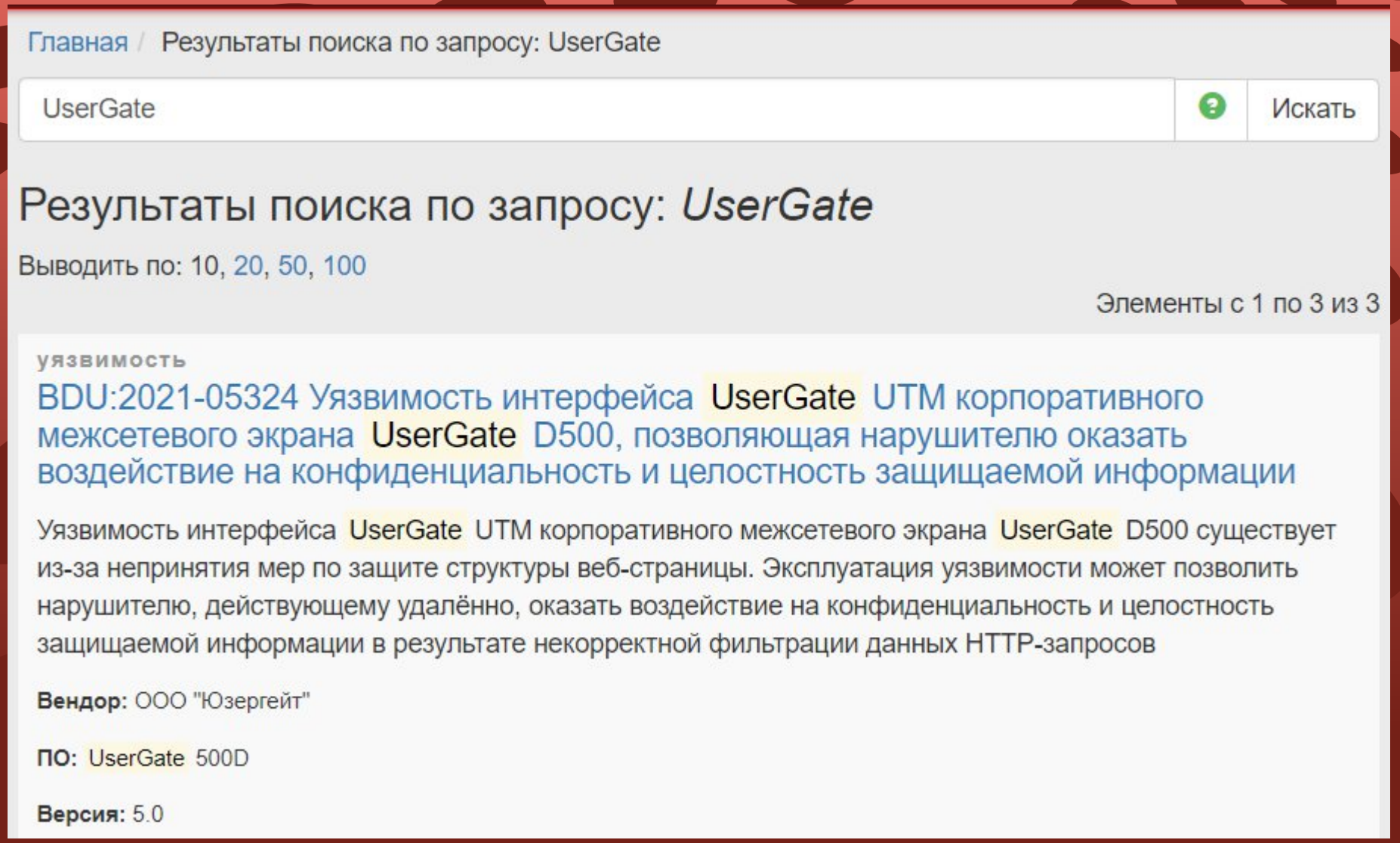
https://www.comnews.ru/content/231469/2024-02-08/2024-w06/1008/rynok-ngfw-rossii-podnimetsya-no-vyzhivut-nem-ne-vse

В конечном итоге, за киберустойчивость компании отвечает не вендор

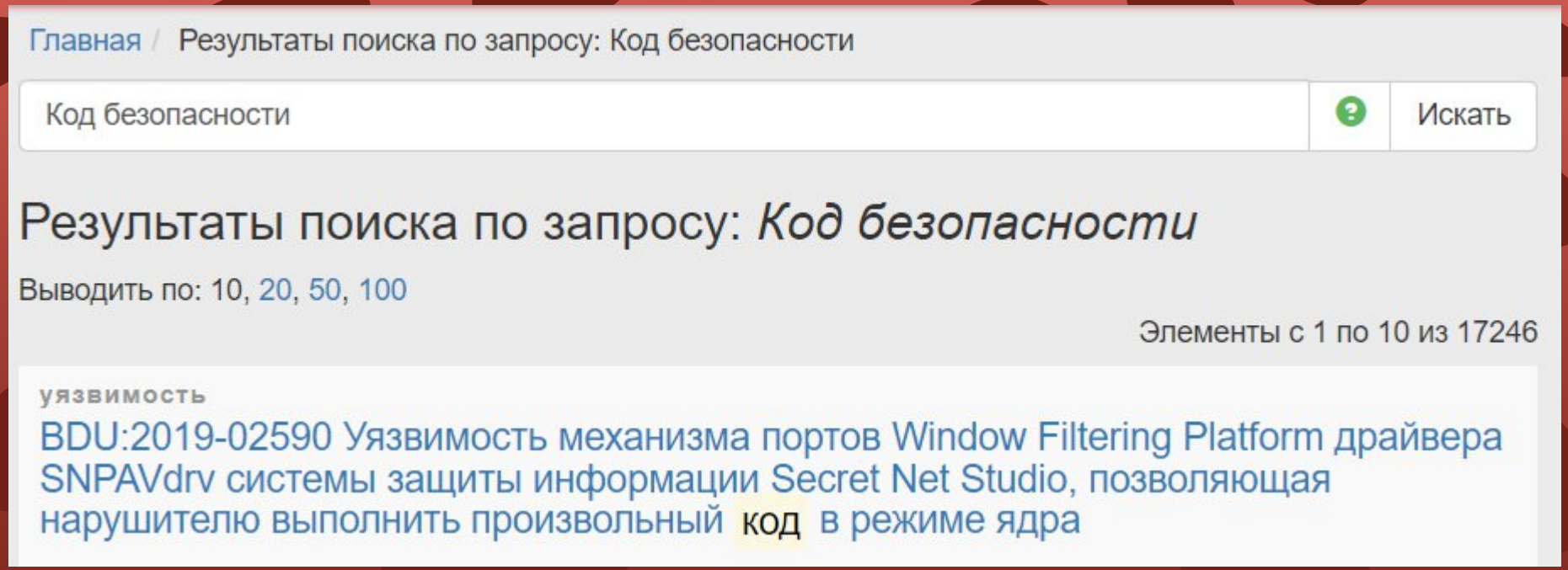
Управление уязвимостями: классика


Главная / Результаты поиска по запросу: Eltex
Eltex
Искать
Результаты поиска по запросу: Eltex
Выводить по: 10, 20, 50, 100
Элементы с 1 по 5 из 5
уязвимость
BDU:2019-02713 Уязвимость веб-сервера коммутаторов Eltex , позволяющая нарушителю вызвать отказ в обслуживании
Уязвимость веб-сервера коммутаторов Eltex существует из-за отсутствия проверки длины параметров

У нас нет CVE


Главная / Результаты поиска по запросу: UserGate
UserGate
Искать
Результаты поиска по запросу: UserGate
Выводить по: 10, 20, 50, 100
Элементы с 1 по 3 из 3
уязвимость
BDU:2021-05324 Уязвимость интерфейса UserGate UTM корпоративного межсетевого экрана UserGate D500, позволяющая нарушителю оказать воздействие на конфиденциальность и целостность защищаемой информации
Уязвимость интерфейса UserGate UTM корпоративного межсетевого экрана UserGate D500 существует из-за непринятия мер по защите структуры веб-страницы. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, оказать воздействие на конфиденциальность и целостность защищаемой информации в результате некорректной фильтрации данных HTTP-запросов
Вендор: ООО "Юзергейт"
ПО: UserGate 500D
Версия: 5.0

Совсем нет



Ну хоть у кого-то есть

Наличие годного коммерческого сканера уязвимостей – новая гигиеническая норма

Управление уязвимостями: сейчас

~~(Публикация уязвимости)~~

Сканирование

Анализ актуальности, поиск информации об эксплойтах

Стендирование, выработка тех. рекомендаций

Возможно, запрос вендору на закрытие уязвимости (но без особой надежды)

Установка обновления

Проверка сканером

Обзор рынка NGFW в 2024г.

https://habr.com/ru/articles/832464/

69*

производителей NGFW в РФ

Надо просто делать все, что можем
дожидаясь
зрелости лидеров рынка