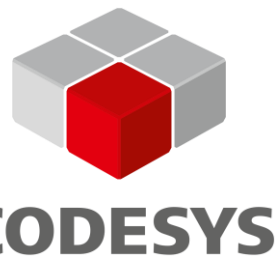
kaspersky

Технологический суверенитет со стороны кибербезопасности

Артем Зиненко

Лаборатория Касперского

PRO автоматизацию

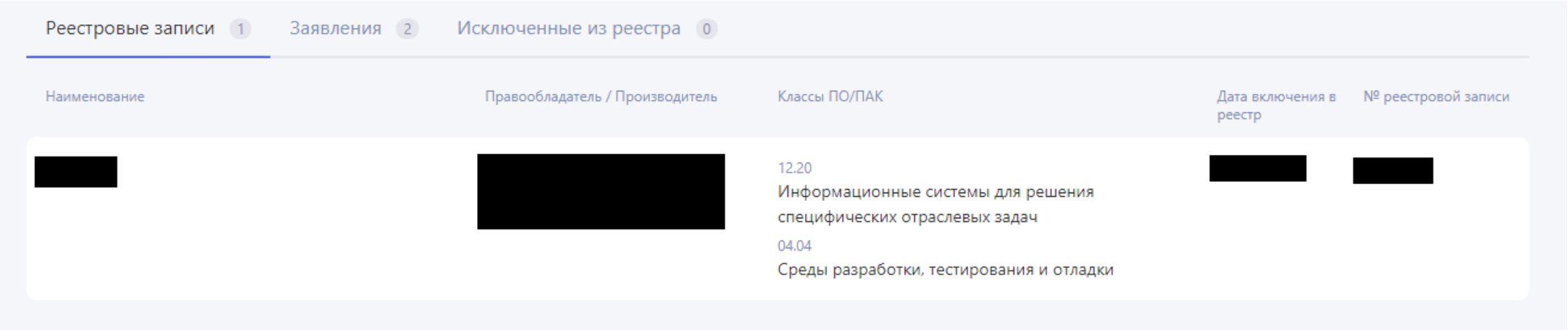


Примеры, как не нужно делать

Все ли продукты в Реестре[1] - российские?

[1] Реестр российского ПО https://reestr.digital.gov.ru/

Запись в Реестре российского ПО



Запись в Реестре российского ПО

Об установлении **запрета** на допуск программного обеспечения, происходящего из **иностранных** государств

[redacted]

[redacted]

12.20
Инфор
специо
0 04
Среды

[redacted]

СТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ № [redacted]

Москва

О формировании и ведении единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации

В соответствии с пунктами 25, 26 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (далее – Правила), и на основании решения Экспертного совета по программному обеспечению при Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Экспертный совет) от 31 мая 2021 г.

Анализ продукта


```
$ head -n10 ./ReadmeP006.txt
================================================================
Patch P006 "DECEMBER-2021" for WinCC OA Version 3.18      December 2021
================================================================


Summary:
========

 Enhancements and bugfixes for WinCC OA.
```

Siemens SIMATIC WinCC OA

Известные уязвимости Siemens

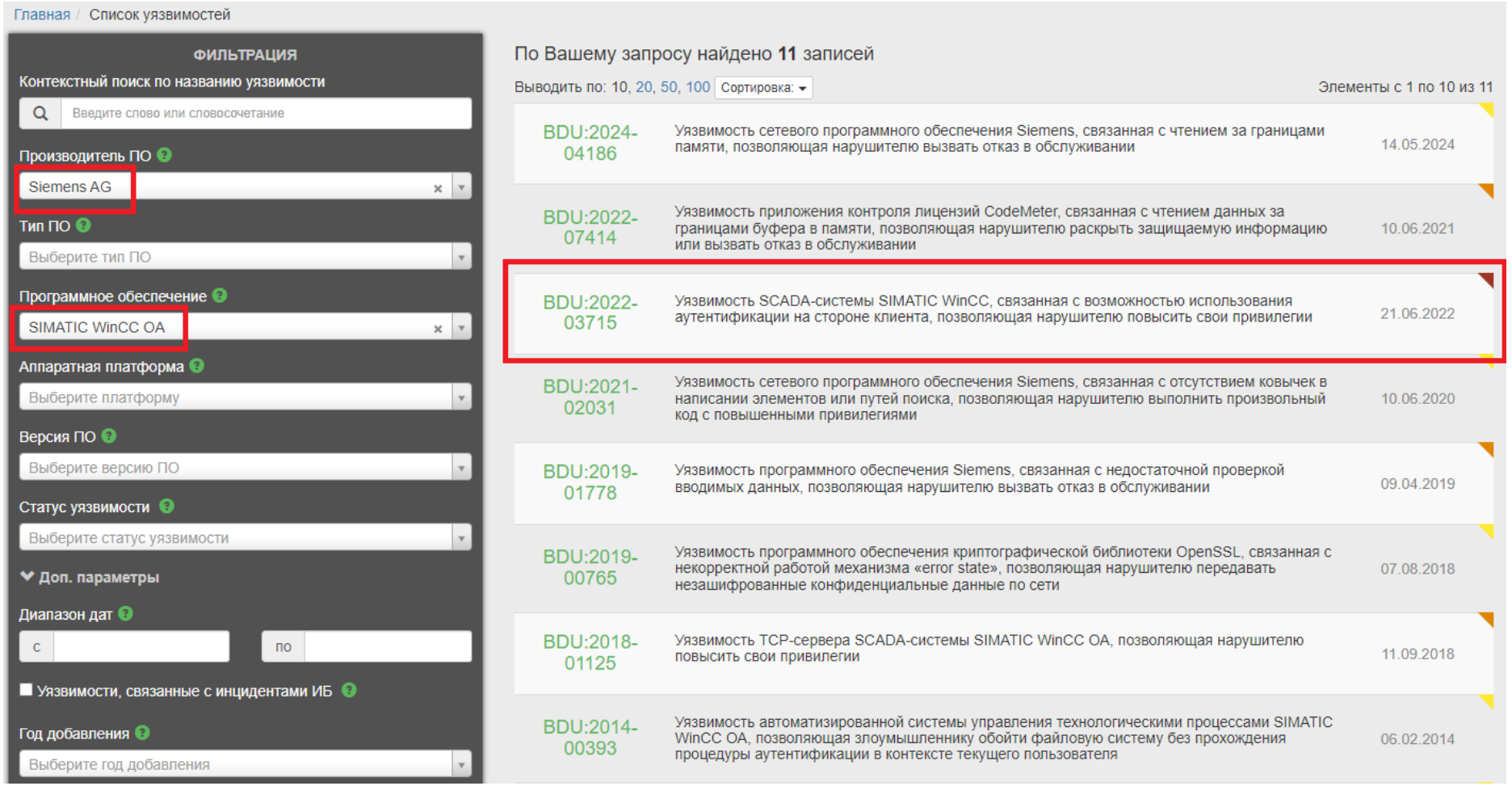
CVE-2022-33139, CVSSv3: 9.8

The following versions of SIMATIC WinCC OA, a SCADA HMI system, are affected:

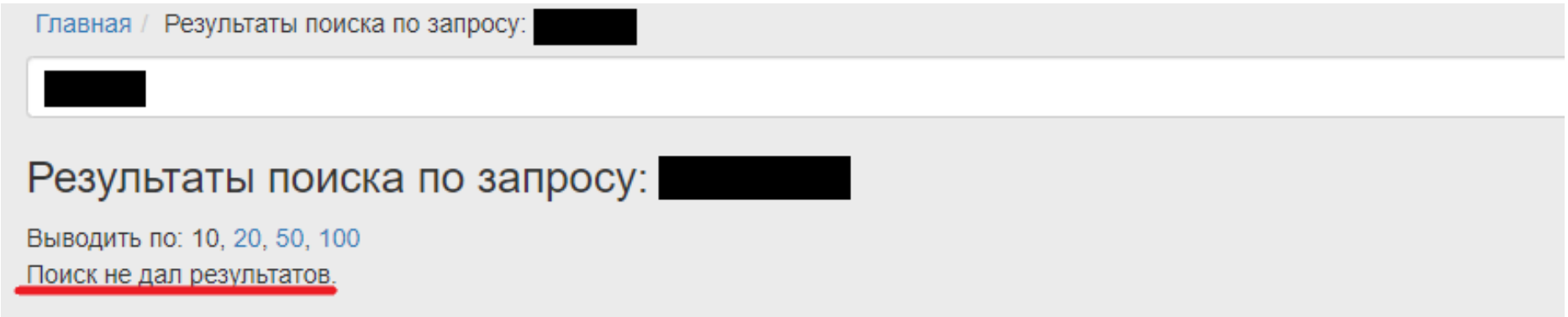
- SIMATIC WinCC OA v3.16: All versions
- SIMATIC WinCC OA v3.17: All versions
- **SIMATIC WinCC OA v3.18: All versions**

Источник: https://cert-portal.siemens.com/productcert/pdf/ssa-111512.pdf

Известные уязвимости Siemens в БДУ ФСТЭК



Известные уязвимости вендора в БДУ ФСТЭК



Насколько импортонезависимый продукт независим от импорта?

Импортонезависимый продукт?

Программное обеспечение блока внесено в реестр отечественного ПО.

Операционная система на базе ядра Linux.

Аппаратная часть выполнена на импортонезависимой электронно-компонентной базе (материковый Китай).

материковый Китай

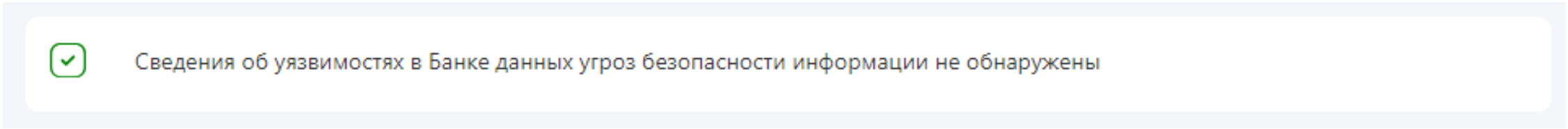
История одной уязвимости

Общение с вендором

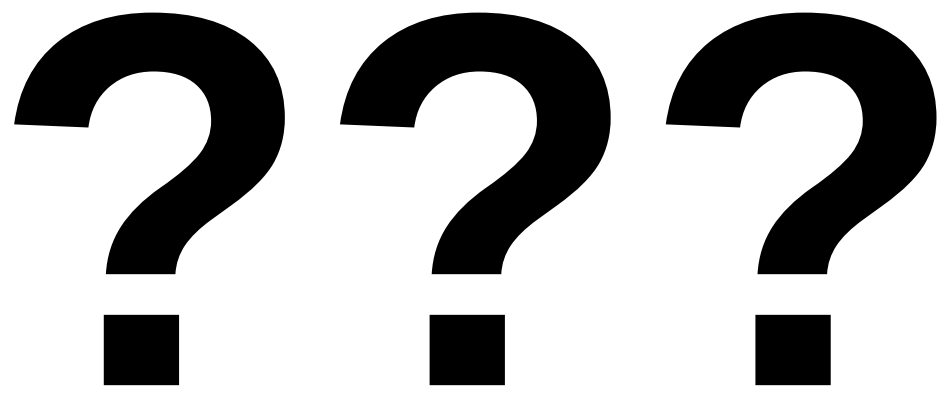
Based on our internal risk assessment, … we have decided ***not to publish any fix*** *for the listed issues …*

Нет известных уязвимостей – продукт защищённый?

Нет известных уязвимостей для продукта в БДУ



Аудит продукта



потратили на поиск **критической уязвимости** в продукте
(удаленное выполнение произвольного кода)

Аудит продукта

1 час

потратили на поиск **критической уязвимости** в продукте
(удаленное выполнение произвольного кода)

Информация о новых уязвимостях

Подход большинства вендоров

Что делать?

Что делать вендорам?

- **Внедрять** современные практики **безопасной разработки**
- **Проводить** регулярный **аудит** безопасности своих продуктов
- **Уведомлять пользователей** продуктов о проблемах в безопасности
- **Управлять** уязвимостями в используемых **внешних компонентах**
- Создать канал для **приема информации** о проблемах в безопасности от **внешних исследователей**

Что делать компаниям?

- При выборе новых продуктов уделять внимание **уровню зрелости** вендора с точки зрения безопасности
- **Проводить** независимый **аудит** безопасности используемых продуктов
- **Управлять уязвимостями** в используемых продуктах
- При внедрении требовать **передачи** всех **артефактов**, необходимых для **работы** продукта
- Выстраивать **архитектуру** систем с использованием подходов **эшелонированной защиты** (Defense in Depth) и **нулевого доверия** (Zero Trust)

Положительные изменения

Спасибо за внимание!

kaspersky

Артем Зиненко

Artem.Zinenko@kaspersky.com

PRO автоматизацию