

Собираем информацию по безопасности от инструментов DevSecOps

Всё через одно место

Павел
Василевич

Security
Team Lead

Plesk

О себе



15 лет в Plesk:

- PHP разработчик
- C++ разработчик
- Windows Team Lead
- DevOps Team Lead

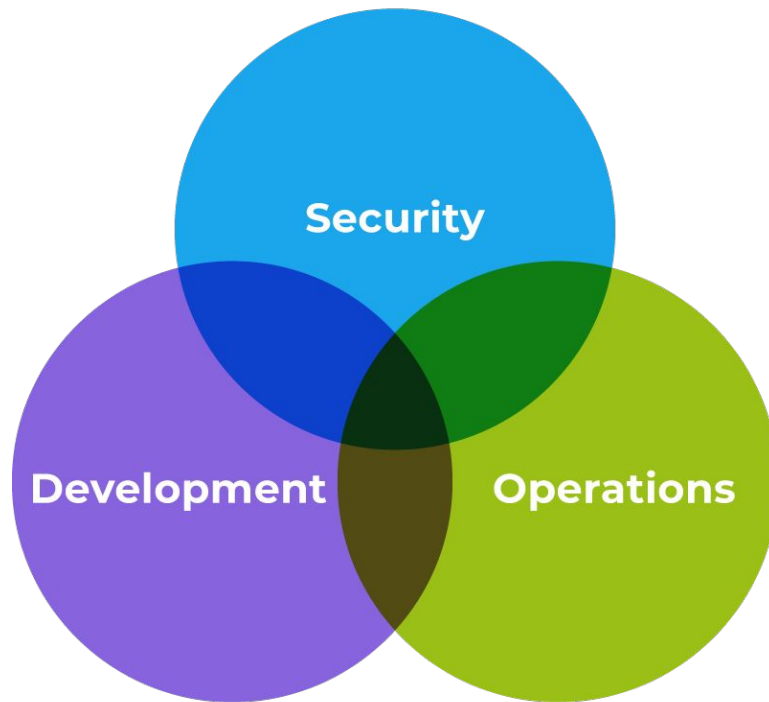
Сейчас:

- **Security Team Lead**

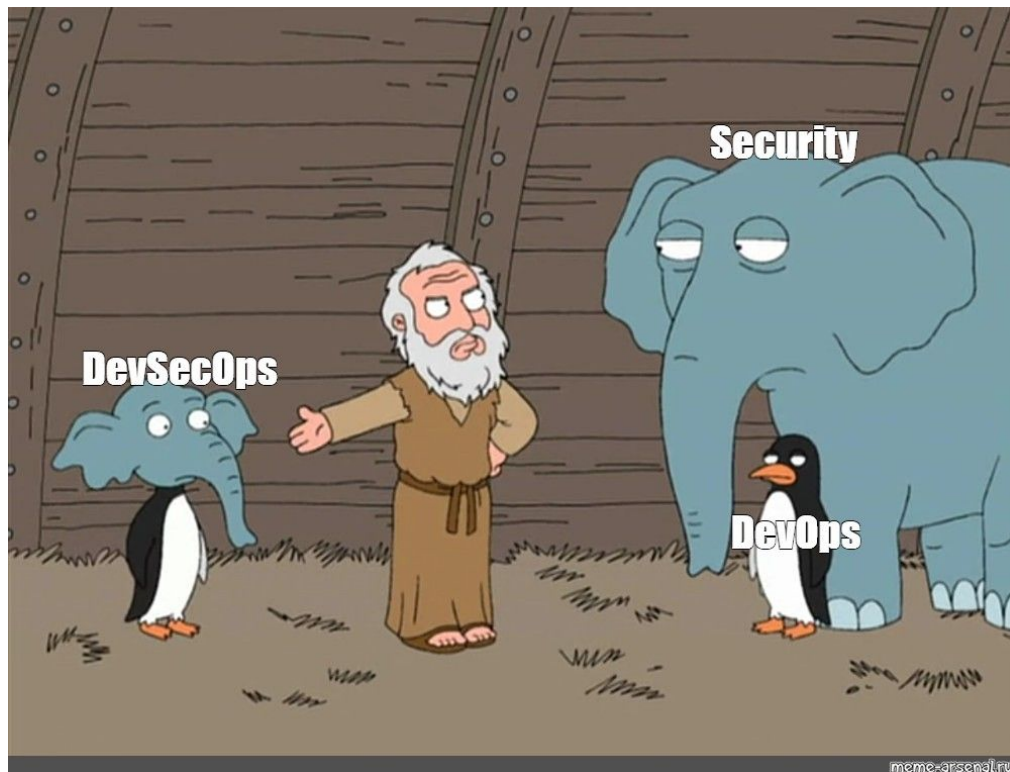


- 380 000 серверов
- 11+ миллионов сайтов
- 6% мирового интернета*

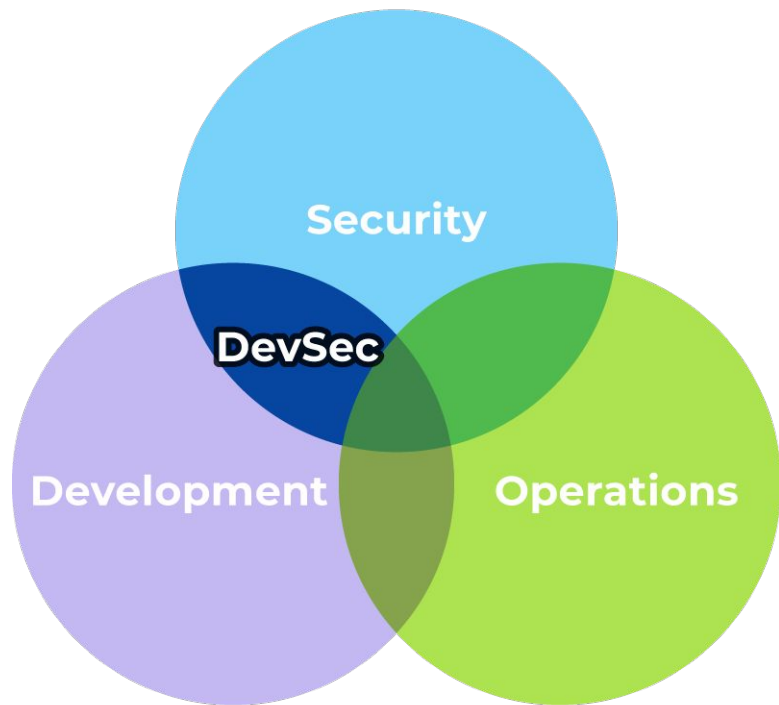
Что такое DevSecOps?



Почему DevSecOps?

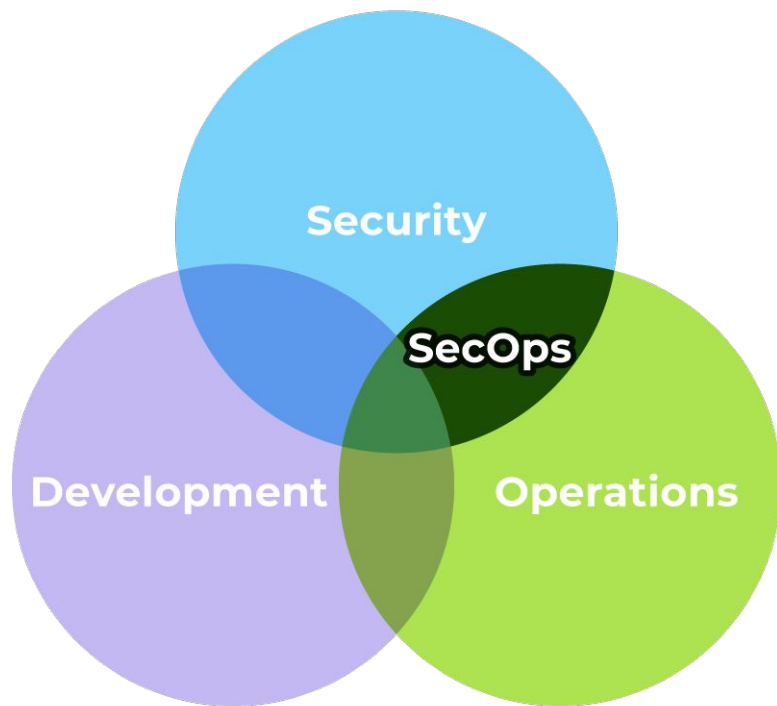


DevSec



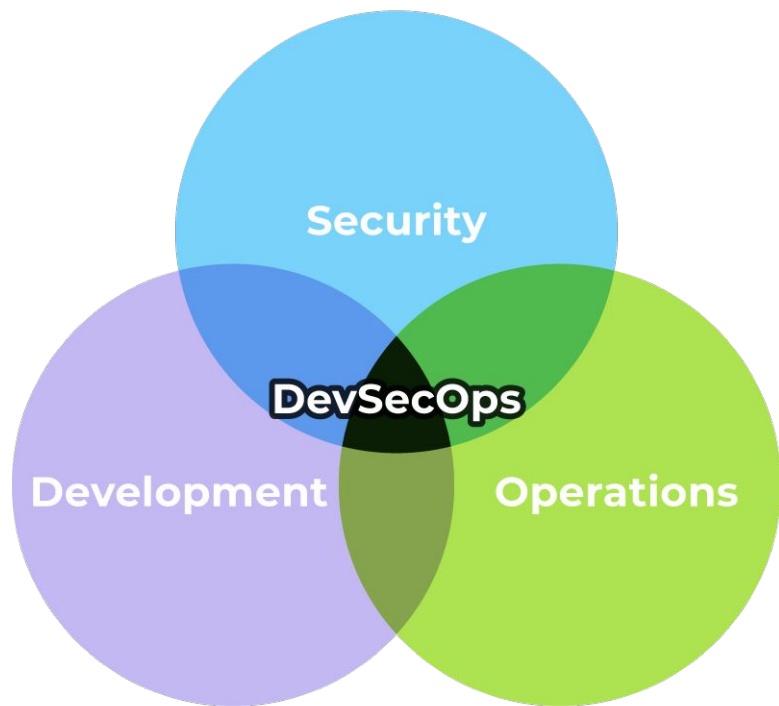
- Работа с требованиями
- Моделирование угроз
- Разработка
- Тестирование

SecOps



- Инфраструктура
- Мониторинг
- Инциденты

DevSecOps



- Процессы
- Культура

DevSec

Зависимости
Уязвимости
Секреты

SecOps

Инфраструктура
Облака
Контейнеры

DevSecOps

DefectDojo

DevSec

Зависимости

Уязвимости

Секреты

SecOps

Инфраструктура

Облака

Контейнеры

DevSecOps

DefectDojo

Пример: Библиотеки в Go

go.mod:

```
require (  
    ...  
    github.com/mholt/archiver v3.1.1  
)
```

service.go:

```
archiver.Unarchive(archivePath, dstPath)
```

is-ten-thousand

0.2.0 • Public • Published a year ago



Readme



Explore

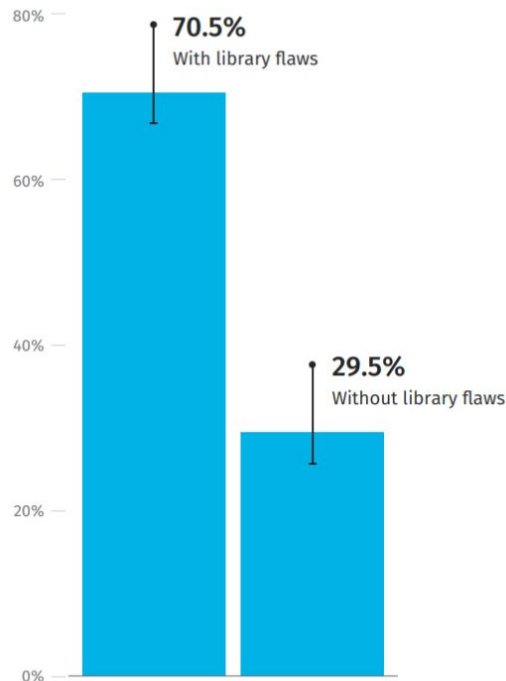
BETA

is-ten-thousand

If you need to know if a number is ten thousand.

Источник: <https://www.npmjs.com/package/is-ten-thousand>

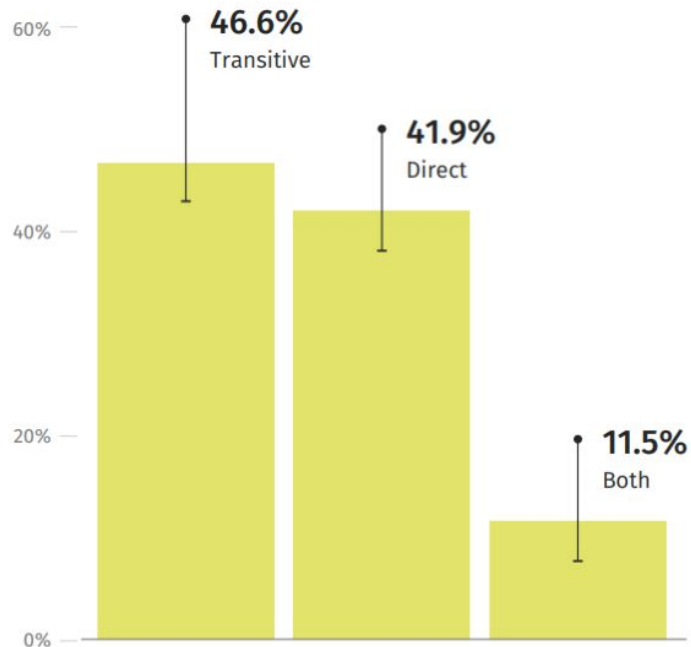
Уязвимости в зависимостях



Источник: <https://www.veracode.com/sites/default/files/pdf/resources/reports/state-of-software-security-open-source-edition-veracode-report.pdf>

- 70.5% приложений содержат уязвимости в зависимостях

Транзитивные зависимости



- 46.6% - транзитивные
- 41.9% - прямые

Источник: <https://www.veracode.com/sites/default/files/pdf/resources/reports/state-of-software-security-open-source-edition-veracode-report.pdf>

GitHub рекомендует

Code
Fest



01

Check your dependencies for vulnerabilities regularly.

The first step is knowing, and you can't patch what you don't know about. For people here

Источник: <https://octoverse.github.com/static/github-octoverse-2020-security-report.pdf>

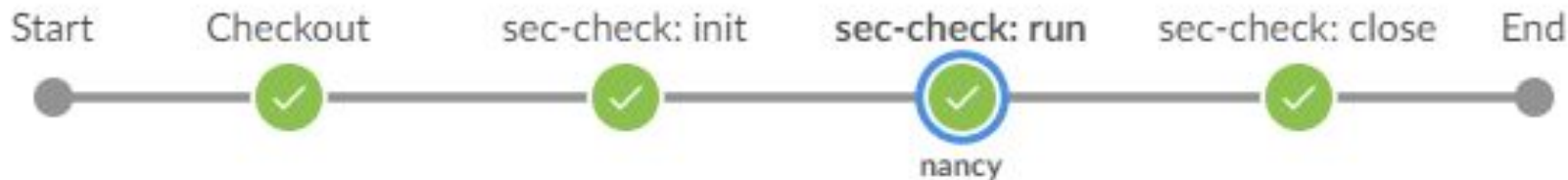
Инструменты: зависимости в GO



- Nancy
- OWASP
dependency-check

Источник: <https://github.com/sonatype-nexus-community/nancy>

Пример: Jenkins pipeline



```
go list -json -m all |  
docker run --rm -i \  
  sonatypecommunity/nancy:latest sleuth
```

Пример: Результаты сканирования

[CVE-2019-10743] All versions of archiver allow attacker to perform a Zip Slip attack via the "un...

Description

All versions of archiver allow attacker to perform a Zip Slip attack via the "unarchive" functions. It is exploited using a specially crafted zip archive, that holds path traversal filenames. When exploited, a filename in a malicious archive is concatenated to the target extraction directory, which results in the final path ending up outside of the target folder. For instance, a zip may hold a file with a ".././file.exe" location and thus break out of the target folder. If an executable or a configuration file is overwritten with a file containing malicious code, the problem can turn into an arbitrary code execution issue quite easily.

OSS Index ID

96fbd898-c476-48c5-8972-848f84403e92

CVSS Score

5.5/10 (Medium)

CVSS Vector

CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

Link for more info

<https://ossindex.sonatype.org/vulnerability/96fbd898-c476-48c5-8972-848f84403e9>

Куда встраивать проверки?

- IDE разработчика
- Continuous Integration (CI)
- Запуски по расписанию



Как обрабатывать результаты?

- Останавливаем CI pipeline
- Или нет?



DevSec

Зависимости

Уязвимости

Секреты

SecOps

Инфраструктура

Облака

Контейнеры

DevSecOps

DefectDojo

Мысли вслух...

Code
Fest





OWASP TOP 10

Open Web Application
Security Project

Источник: <https://owasp.org/www-project-top-ten/>



SANS 25

SysAdmin, Audit, Network,
and Security

Источник: <https://www.sans.org/top25-software-errors/>

Обучение



Kontra

Developer First Application
Security Training

Источник: <https://application.security/free/owasp-top-10>



Root-Me

The fast, easy, and affordable way to train your hacking skills.

Источник: <https://www.root-me.org/>

Инструменты: SAST

- Static application security testing
- Сканируем код
 - Проверки по паттернам (SemGrep, SonarQube, ...)
 - Анализ потока выполнения (коммерческие решения)

Инструменты: DAST

- Dynamic Application Security Testing
- Важна гибкость / возможность кастомизации
- Важно умение работать с динамическими сайтами (JS)

DevSec

Зависимости
Уязвимости
Секреты

SecOps

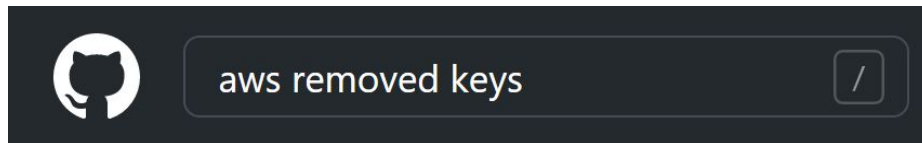
Инфраструктура
Облака
Контейнеры

DevSecOps

DefectDojo

GitHub и AWS ключи

Code
Fest



11,484 commit results

Sort: Best match ▾

shahriarkasib/WaferEndtoEnd

aws key removed

shahriarkasib committed 14 hours ago ✓



50ec80c



Rahul-Barick/docker-react

Removed secure aws keys

Rahul-Barick committed 3 days ago ✗



52234d1



Если GIT сервер локальный?

- Нет автоматического отслеживания
- Ключ расползется по машинкам
- Ошибка или уязвимость могут вскрыть проблему
- Не забывайте про историю в GIT



Инструменты: поиск секретов

```
{  
  "branch": "origin/master",  
  "commit": "TECH Reorganize config files\n",  
  "commitHash": "4466e22dabd9a7a0dbf1280a48c",  
  "date": "2020-07-09 05:11:23",  
  "diff": "@@ -1,14 +1,10 @@\n APP_ENV=devel",  
  "path": ".env.e2e",  
  "printDiff": "@@ -1,14 +1,10 @@\n APP_ENV=",  
  "reason": "High Entropy",  
  "stringsFound": [  
    "KEY=cgH5BSgNdML1b0...",  
    "ID=0Eibqb3GNxlFEf...",  
    "KEY=2OV56vuT4LFdR...",  
    "KEY=cgH5BSgNdML1b0..."  
  ]  
}
```

- TruffleHog
- GitLeaks
- Talisman
- SemGrep

DevSec

Зависимости
Уязвимости
Секреты

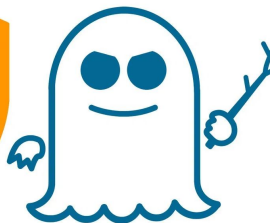
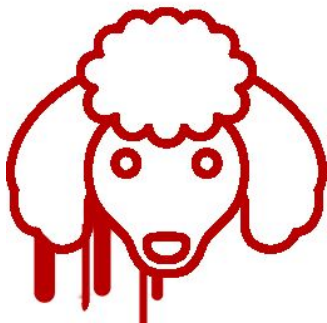
SecOps

Инфраструктура
Облака
Контейнеры

DevSecOps

DefectDojo

Инфраструктура уязвима



Источник: логотипы уязвимостей DirtyCow, HeartBleed, ShellShock, Poodle, Meltdown, Spectre

Инструменты: сетевые сканеры

- Большой выбор:
 - Бесплатные: NMap, OpenVas, ...
 - Коммерческие
- Регулярное сканирование



DevSec

Зависимости
Уязвимости
Секреты

SecOps

Инфраструктура
Облака
Контейнеры

DevSecOps

DefectDojo

Облака

Code
Fest



Google Cloud



Microsoft Azure

Источник: <https://cloud.google.com/> <https://aws.amazon.com/> <https://azure.microsoft.com/>

Инструменты: Аудит в облаках

- ScoutSuite
- CloudSploit



toniblyx/my-arsenal-of-aws-security-tools

Источник: <https://github.com/toniblyx/my-arsenal-of-aws-security-tools>

Инструменты: Аудит в AWS



- CIS AWS Benchmarks
- GDPR
- HIPAA
- PCI-DSS, ISO-27001, ...

Источник: <https://github.com/toniblyx/prowler>

Инструменты: Prowler

```
~/Downloads/prowler$ ./prowler

[PROWLER] v2.4.0-07042021
the handy cloud security tool

Date: Thu Apr  8 00:25:47 CEST 2021

Colors code for results:
INFO (Information), PASS (Recommended value), WARNING (Ignored by whitelist), FAIL (Fix required), Not Scored

This report is being generated using credentials below:

AWS-CLI Profile: [ENV] AWS API Region: [eu-west-1] AWS Filter Region: [all]
AWS Account: [ ] UserId: [AROAS5235KJ ]
Caller Identity ARN: [arn:aws:sts:: :assumed-role/ ]

1.0 Identity and Access Management - CIS only - [group1] *****
0.1 Generating AWS IAM Credential Report...
1.1 [check11] Avoid the use of the root account (Scored)
    PASS! Root user in the account wasn't accessed in the last 1 days
1.2 [check12] Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Scored)
    FAIL! User test3 has Password enabled but MFA disabled
1.3 [check13] Ensure credentials unused for 90 days or greater are disabled (Scored)
    FAIL! User test2 has never logged into the console since creation and their password not changed in the past 90 days
```

Источник: <https://github.com/toniblyx/prowler>

DevSec

Зависимости
Уязвимости
Секреты

SecOps

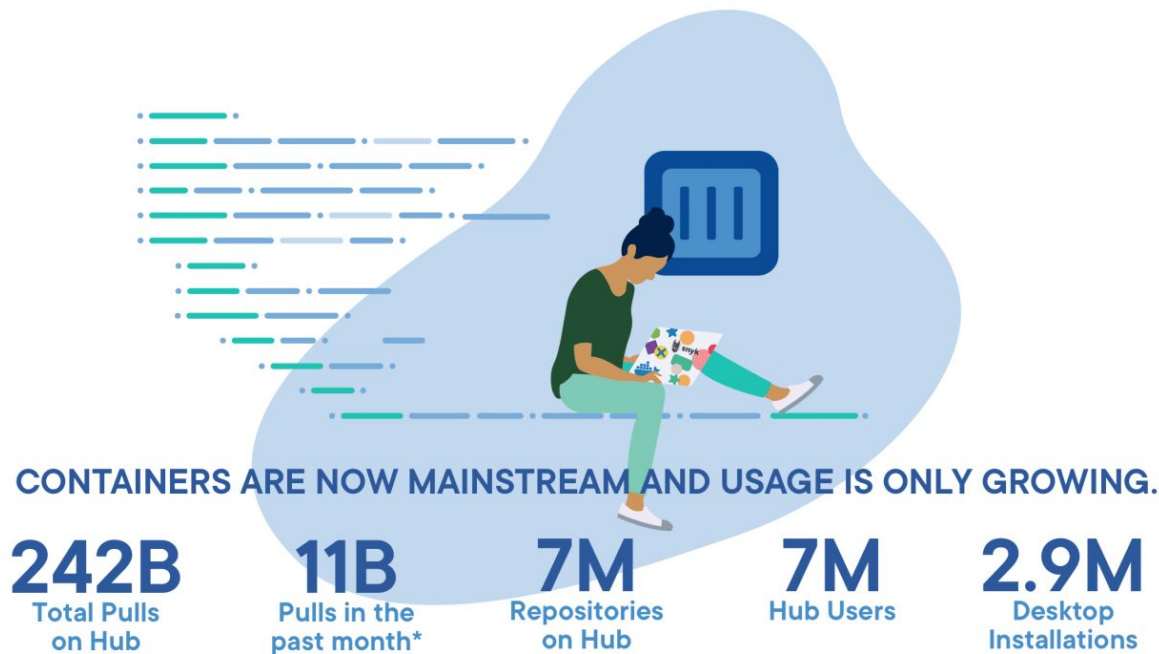
Инфраструктура
Облака
Контейнеры

DevSecOps

DefectDojo

Безопасность контейнеров

Code
Fest



Источник: <https://snyk.io/learn/container-security/>

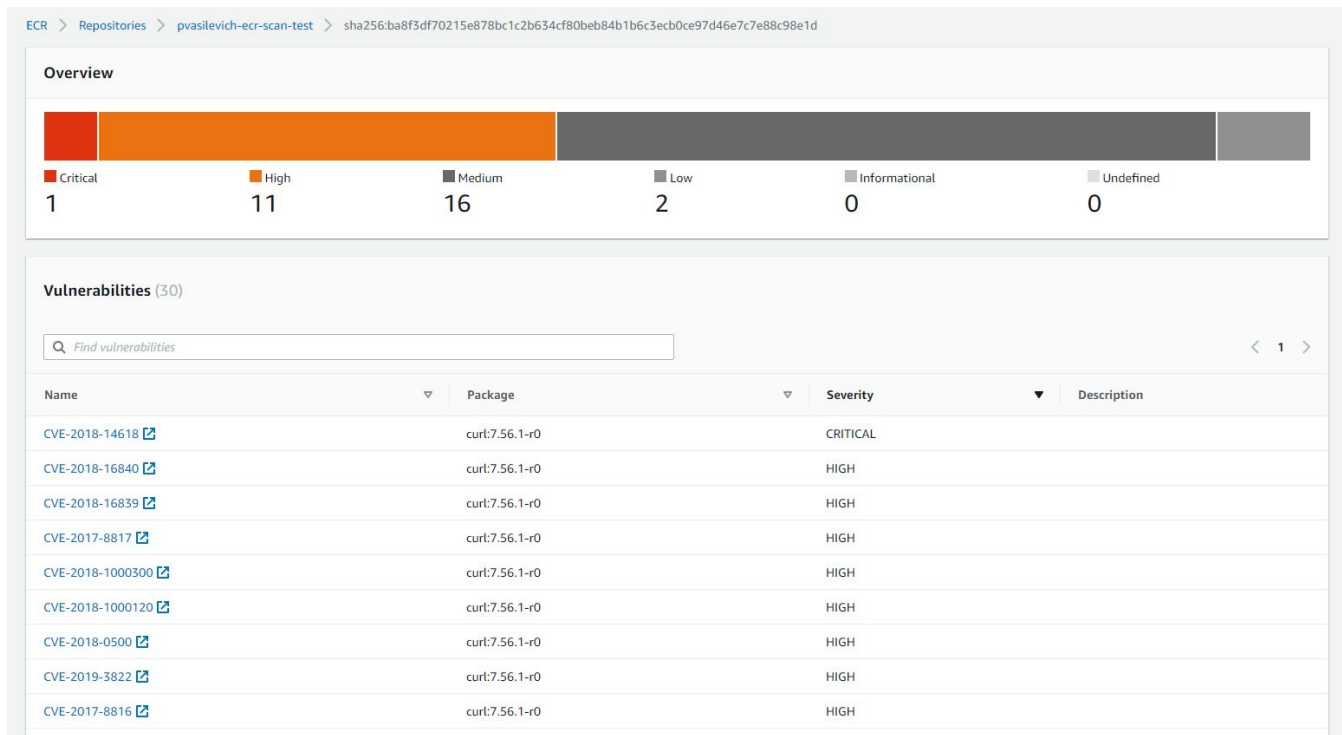
*UP FROM 5.5B A YEAR AGO

Инструменты: скан образов

- Trivy
- Clair
- Anchore

Инструменты: AWS ECR scan

Code
Fest



DevSec

Зависимости
Уязвимости
Секреты

SecOps

Инфраструктура
Облака
Контейнеры

DevSecOps

DefectDojo

Проблемы роста

- Множество решений
- Информация от инструментов разрознена
- У каждого решения свой формат и интерфейс
- Нет сквозной приоритезации
- Нет полной картины



DefectDojo

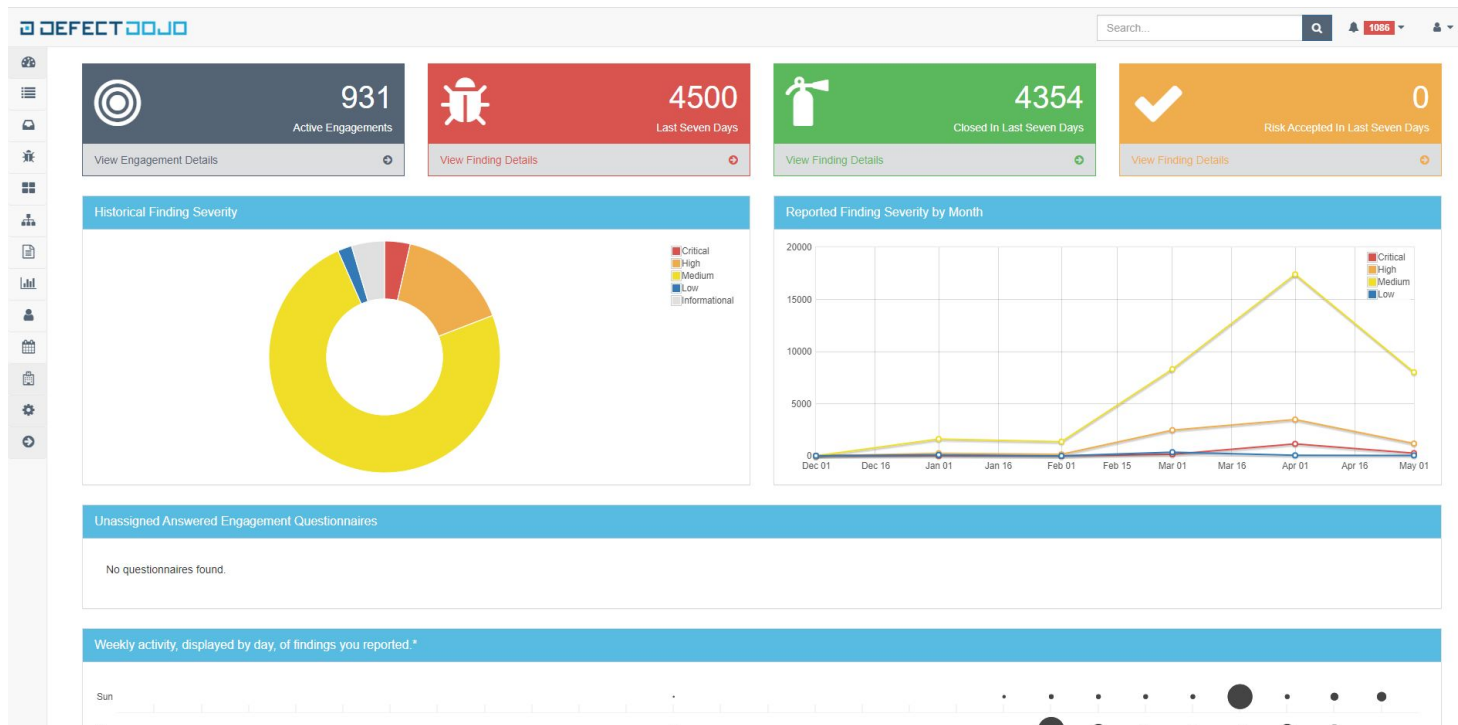


- Open-source
- OWASP flagship project
- Альтернативы:
 - Faraday, SecureCodeBox, ArcherySec, ThreadFix, Nucleus, AppSec.Hub

Источник: <https://www.defectdojo.org/>

DefectDojo

Code
Fest



Products

Code
Fest

The screenshot displays the DefectDojo web application interface. The top navigation bar includes the DefectDojo logo, a search bar, and notification icons for 999 alerts. The left sidebar contains a menu with icons for Overview, Components, Metrics, Engagements, Findings, Endpoints, Benchmarks, and Settings. The main content area is titled 'Overview' and shows details for a product named 'Self Care Portal'. The 'Metrics' section displays a bar chart with counts for Critical (2), High (6), Medium (4), Low (5), Informational (0), and Total (17). The 'Technologies' section indicates no technologies are listed. The 'Regulations (1)' section lists 'GDPR EU & EU Data Extra-Territorial Applicability'. The 'Benchmark Progress' section indicates no benchmarks are listed. The right sidebar contains sections for 'Metadata' (Business Criticality: Very High, Product Type: Plesk online services, Platform: Web, Lifecycle: Production, Origin: Internally Developed, User Records: Not Specified, Revenue: Not Specified), 'Custom Fields' (Confluence: https://docs.plesk.ru/en/ru/18.0/faq/faq-fresh-install), 'Contacts' (Team Manager: Alexey Tikhonov, Product Manager: (empty), Technical Contact: Andrey Nagayev, Authorized Users: alexey.tikhonov, andrey.nagayev), and 'Notifications' (Engagement added: Slack, Mail, Alert; Close engagement: Slack, Mail, Alert).

DEFECTDOJO

Search...

My Product [A] [2023]

Overview Components Metrics Engagements 4 Findings 18 Endpoints 2 Benchmarks Settings

Description

Self Care Portal

Metrics

2 CRITICAL 6 HIGH 4 MEDIUM 5 LOW 0 INFORMATIONAL 17 TOTAL

Technologies

There are no technologies.

Regulations (1)

GDPR EU & EU Data Extra-Territorial Applicability Privacy

Benchmark Progress

There are no benchmarks

Metadata

Business Criticality Very High

Product Type Plesk online services

Platform Web

Lifecycle Production

Origin Internally Developed

User Records Not Specified

Revenue Not Specified

Custom Fields

Confluence https://docs.plesk.ru/en/ru/18.0/faq/faq-fresh-install

Contacts

Team Manager Alexey Tikhonov (alex.tikhonov)

Product Manager (empty)

Technical Contact Andrey Nagayev (andrey.nagayev)

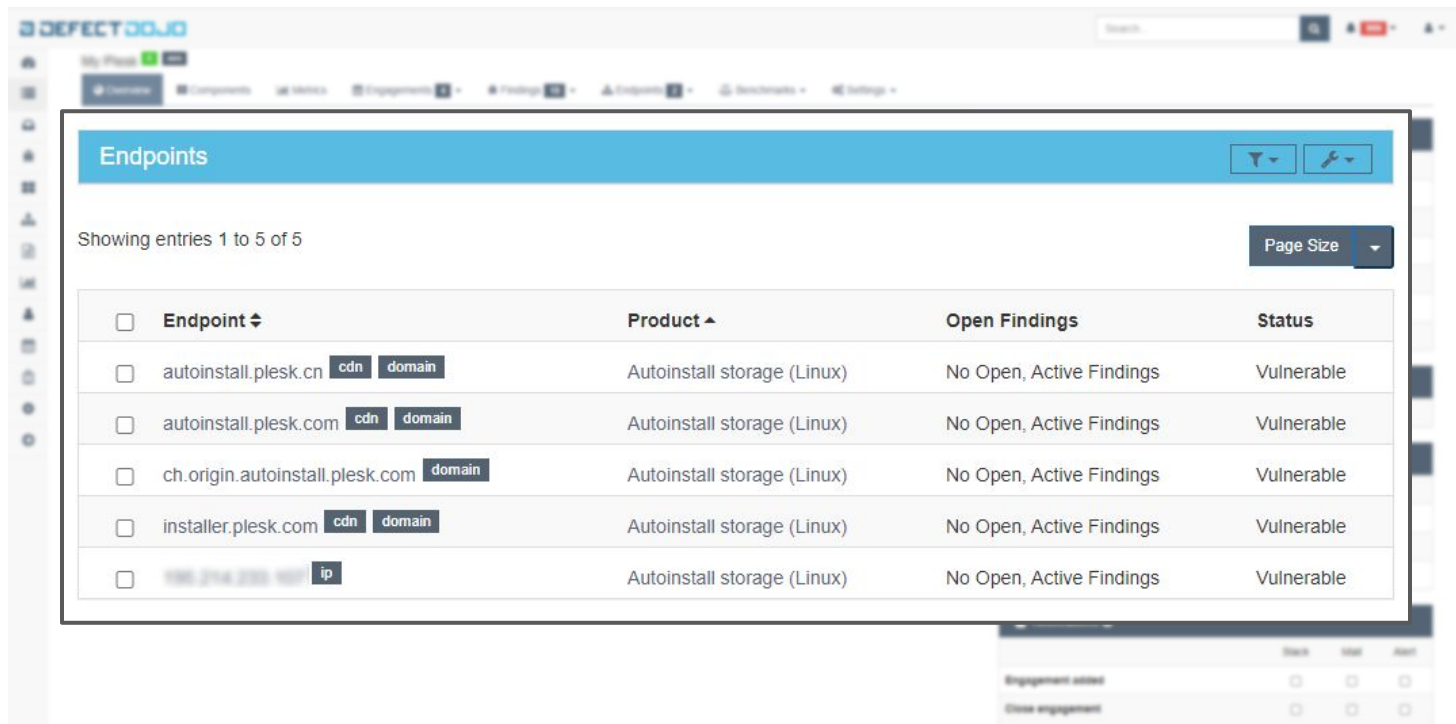
Authorized Users alexey.tikhonov, andrey.nagayev

Notifications

	Slack	Mail	Alert
Engagement added	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Close engagement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Products

Code
Fest



The screenshot shows the DefectDojo web interface. The top navigation bar includes 'My Place', 'Components', 'Metrics', 'Engagements', 'Findings', 'Endpoints', 'Benchmarks', and 'Settings'. The 'Endpoints' tab is selected. Below the navigation bar, there's a blue header for 'Endpoints' with filter and edit icons. The main content area shows 'Showing entries 1 to 5 of 5' and a 'Page Size' dropdown. A table lists five endpoints, all with 'Vulnerable' status and 'No Open, Active Findings'.

<input type="checkbox"/>	Endpoint ↕	Product ▲	Open Findings	Status
<input type="checkbox"/>	autoinstall.plesk.cn cdn domain	Autoinstall storage (Linux)	No Open, Active Findings	Vulnerable
<input type="checkbox"/>	autoinstall.plesk.com cdn domain	Autoinstall storage (Linux)	No Open, Active Findings	Vulnerable
<input type="checkbox"/>	ch.origin.autoinstall.plesk.com domain	Autoinstall storage (Linux)	No Open, Active Findings	Vulnerable
<input type="checkbox"/>	installer.plesk.com cdn domain	Autoinstall storage (Linux)	No Open, Active Findings	Vulnerable
<input type="checkbox"/>	198.214.202.100 ip	Autoinstall storage (Linux)	No Open, Active Findings	Vulnerable

Products

Code
Fest

The screenshot shows the DefectDojo web application interface. The top navigation bar includes the DefectDojo logo, a search bar, and several menu items: My Place, Overview, Components, Metrics, Engagements, Findings, Endpoints, Benchmarks, and Settings. The main content area is titled 'Description' and shows a 'Get Code' button. A dropdown menu for 'Business criticality' is open, displaying a list of options: Very High, High, Medium, Low, Very Low, and None. The 'Very High' option is currently selected and highlighted in blue. Below the dropdown, the 'Origin' field is visible with the value 'Internally Developed'. On the right side of the page, there are sections for 'Metadata' (Business Criticality: Very high, Product Type: PaaS online services), 'Technical Content', 'Authorized Users', and a 'Notifications' table with columns for Stock, Mail, and Alert.

Business criticality
Very High
High
Medium
Low
Very Low
None

Notifications	Stock	Mail	Alert
Engagement added	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Close engagement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Products

Code
Fest

The screenshot shows the DefectDojo web application interface. The top navigation bar includes the DefectDojo logo, a search bar, and user profile information. The main content area is titled 'Products' and features a sidebar with navigation links like 'Overview', 'Components', 'Metrics', 'Engagements', 'Findings', 'Endpoints', 'Benchmarks', and 'Settings'. The 'Lifecycle' dropdown menu is open, showing options: 'Production' (selected), 'Construction', 'Production' (highlighted in blue), and 'Retirement'. The background shows details for a product named 'WebApp Portal', including its 'Business Criticality' (Very high) and 'Product Type' (Web application services). A table at the bottom right lists notifications for 'Engagement added' and 'Close engagement' with checkboxes for 'Track', 'Mail', and 'Alert'.

Notification	Track	Mail	Alert
Engagement added	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Close engagement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Products

Code
Fest



Products

Code
Fest

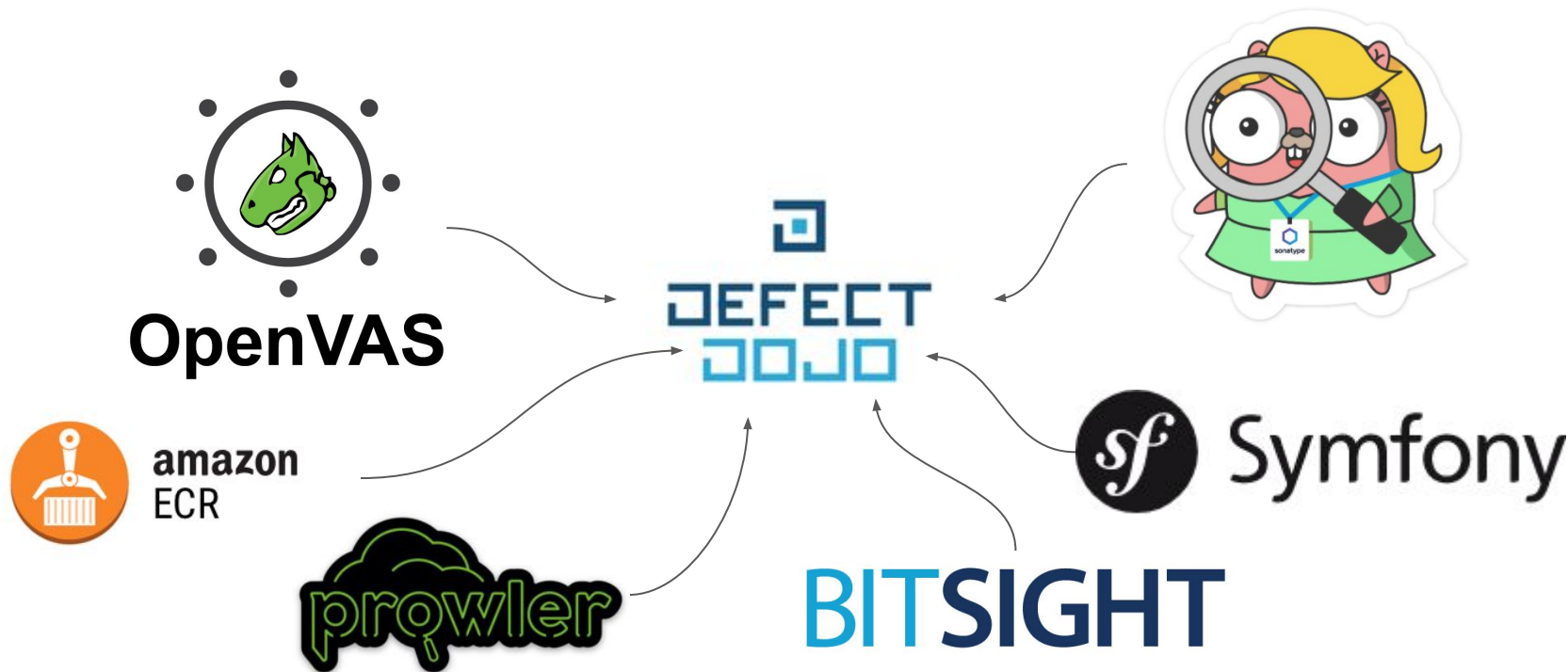
The screenshot shows the DefectDojo web application interface. The 'Products' section is active, displaying a list of products. A modal window titled 'Custom Fields' is open, showing a table with one entry:

Field Name	Field Value
Confluence	https://docs.defectdojo.org/faq/faq-frequently-asked-questions

The background interface includes a sidebar with navigation options like 'Overview', 'Components', 'Metrics', 'Engagements', 'Findings', 'Endpoints', 'Benchmarks', and 'Settings'. The main content area shows product details for 'DefectDojo Product' and a 'Metadata' section with fields like 'Business Criticality' (Very high), 'Product Type' (Product online services), and 'Platform' (Web).

Импорт данных

Code
Fest



Findings

Code Fest

<input type="checkbox"/>	Severity	Name	CWE	CVE	Date	Age	SLA	Reporter	Found By	Status
<input type="checkbox"/>	Critical	zhu-please.com-403 XSS, Configurations: Allow insecure port			Sept. 11, 2020	200	100	Administrator User	Self-Report	Active
<input type="checkbox"/>	Critical	zhu-please.com-403 XSS, Configurations: Allow insecure port			Sept. 11, 2020	200	100	Administrator User	Self-Report	Active
<input type="checkbox"/>	High	version: jenkins/2.1.2 (critical) Remote Code Execution			Oct. 28, 2020	200	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	High	http://www.1.10.0.0 (critical) Denial of Service	400		Oct. 28, 2020	200	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	High	java: 1.10.0 (critical) Denial of Service Request Forgery	918	CVE-2020-28168	Feb. 10, 2021	90	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	High	java: 1.10.0 (critical) Denial of Service Request Forgery	918	CVE-2020-28168	Feb. 10, 2021	90	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	High	nginx: 1.10.0 (critical) Denial of Service Request Forgery	310	CVE-2020-13822	Oct. 28, 2020	200	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	High	node: 10.0.0 (critical) Denial of Service Request Forgery	20	CVE-2020-7720	Oct. 28, 2020	200	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	Medium	nginx: 1.10.0 (critical) Denial of Service Request Forgery	400		Oct. 28, 2020	200	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	Medium	zhu-please.com-403 Web Application Headers: Missing response			Sept. 11, 2020	200	100	Administrator User	Self-Report	Active
<input type="checkbox"/>	Medium	zhu-please.com-403 Web Application Headers: Ineffective response			Oct. 28, 2020	200	100	Administrator User	Self-Report	Active
<input type="checkbox"/>	Medium	zhu-please.com-403 Web Application Headers: Ineffective response			Sept. 11, 2020	200	100	Administrator User	Self-Report	Active
<input type="checkbox"/>	Low	nginx: 1.10.0 (critical) Denial of Service Request Forgery	471		Oct. 28, 2020	200	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	Low	nginx: 1.10.0 (critical) Denial of Service Request Forgery	471		Oct. 28, 2020	200	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	Low	nginx: 1.10.0 (critical) Denial of Service Request Forgery	471	CVE-2019-10744	Oct. 28, 2020	200	100	Administrator User	Team Audit	Active
<input type="checkbox"/>	Low	nginx: 1.10.0 (critical) Denial of Service Request Forgery	209	CVE-2020-15125	Oct. 28, 2020	200	100	Administrator User	Team Audit	Active

Findings

Code
Fest

[Overview](#) [Components](#) [Metrics](#) [Engagements](#) 4 [Findings](#) 18 [Endpoints](#) 2 [Benchmarks](#) [Settings](#)

sec-check 2020-10-28 / Yarn audit / serialize-javascript 2.1.2: [#1548] Remote Code Execution / View Finding

serialize-javascript 2.1.2: [#1548] Remote Code Execution Last Reviewed Oct. 28, 2020 by admin, Created Oct. 28, 2020

ID	Severity	SLA	Status	Duplicates	Type	Date discovered	Age	Reporter	CWE	CVE	Found by
13627	High	173	Active	🔍🔍🔍	Static	Oct. 28, 2020	203 days	admin		None	Yarn audit

Location	Nb occurrences
yarn.lock 🔗	4

Duplicate Cluster (3) ▾

Similar Findings (3) ⓘ ▾ ▾

Description ▴

Advisory URL: <https://npmjs.com/advisories/1548>

`serialize-javascript` prior to 3.1.0 allows remote attackers to inject arbitrary code via the function "deleteFunctions" within "index.js".

An object such as `{ "foo": /1/, "bar": "a\\@_R-<UID>-0_@" }` was serialized as `{ "foo": /1/, "bar": "a\\1/" }`, which allows an attacker to escape the bar key. This requires the attacker to control the values of both foo and bar and guess the value of <UID>. The UID has a keyspace of approximately 4 billion making it a realistic network attack.

The following proof-of-concept calls `console.log()` when the running `eval()`:

```
eval('(' + serialize({ "foo": /1/ + console.log(1)/i, "bar": "@_R-<UID>-0_@" }) + '');
```

Vulnerable Module: `serialize-javascript`
Vulnerable Versions: <3.1.0
Patched Versions: >=3.1.0

Vulnerable Paths:

- `copy-webpack-plugin>serialize-javascript`
- `webpack>terser-webpack-plugin>serialize-javascript`
- `copy-webpack-plugin>serialize-javascript`



DevSec

Зависимости
Уязвимости
Секреты

SecOps

Инфраструктура
Облака
Контейнеры

DevSecOps

DefectDojo

Системный подход к безопасности

Code
Fest

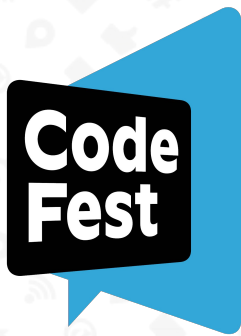


Плюсы для бизнеса



Культура DevSecOps





Спасибо за внимание!

📍 t.me/pvasilevich

🌐 <https://plesk.tech/>

Павел
Василевич

Security
Team Lead

Plesk