



LUNTRY 4.6

**НОВЫЕ ВОЗМОЖНОСТИ ДЛЯ
ЗАЩИТЫ КОНТЕЙНЕРНЫХ И
ОБЛАЧНЫХ СРЕД**



**Дмитрий
Евдокимов**

Founder&CTO Luntry

Обо мне

“

Я не верю в то, что систему можно сделать надежной и безопасной, не понимая того, как она устроена.

”

Основатель
и технический
директор **Luntry**

Более 15 лет опыта в ИБ

Специализация —
безопасность контейнеров
и Kubernetes

Автор ТГ-канала [k8s\(in\)security](#)

Эксперт в сфере безопасности контейнерных сред

- Организатор конференции «БеКон» по БЕзопасности КОНтейнеров
- Бывший редактор рубрик в журнале «ХАКЕР», автор серии статей
- Автор курса «Cloud Native безопасность в Kubernetes»
- Создатель канала k8s (in)security
- Член программного комитета CFP DevOpsConf и KUBER CONF

Спикер

VK Kubernetes
DevOpsConf
Kazhackstan

Confidence
HackInParis
HighLoad++

ZeroNights
KuberConf
OFFZONE

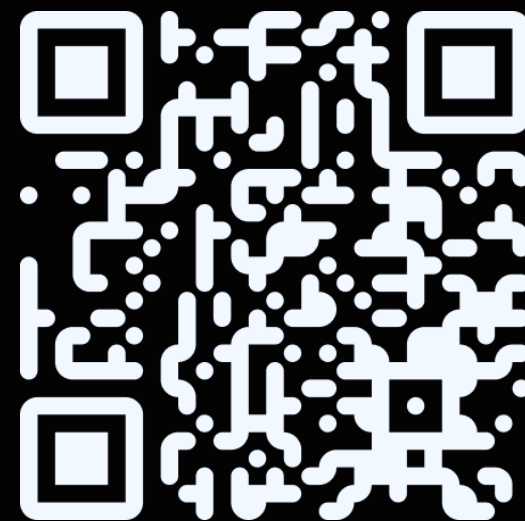
БеКон
BlackHat
DevOops

HITB
PHDays
SAS



О компании Luntry

Luntry — это Комплексная Защита
на всем жизненном цикле
контейнерных приложений
и средств оркестрации на базе Kubernetes



Продукт в реестре Минцифры
<https://reestr.digital.gov.ru/reestr/1057835/>

Получение сертификата ФСТЭК планируется в сентябре 2026 года.

LUNTRY.RU

Регуляторика по контейнеризации и Luntry

ПРИМЕНИМОСТЬ LUNTRY

Защита ГИС и гос. ИС:

- Приказ ФСТЭК № 117 и методический документ от 12.04.26

Защита КИИ:

- 187-ФЗ
- Приказ ФСТЭК № 239 (Приложение)

Защита ИСПДн:

- ФСТЭК № 21 (п.8.11, Приложение)

ОБЯЗАТЕЛЬНОСТЬ

- ГИС: К1, К2, К3
- ИСПДн: У31, У32
- КИИ: да

118 приказ ФСТЭК

Это требование к средам контейнеризации, Luntry это навесное средство защиты и под данный приказ не попадает. НО реализует ряд требований из данного приказа.

117 приказ ФСТЭК и его методический документ

Luntry закрывает пункты про защиту технологий контейнерных сред и их оркестрации (ЗКО) и общие процессы и меры

Информационное сообщение ФСТЭК России 240/24/38

О повышении безопасности средств защиты информации, в состав которых разработчики включают средства контейнеризации или образы контейнеров

Банк данных угроз безопасности информации от ФСТЭК

Luntry закрывает все 5 УБИ посвященные контейнерам

Функциональность Luntry

Контроль
Kubernetes-ресурсов

Контроль состояния Kubernetes-
кластеров

Контроль соответствия кластера
стандартам



Управление безопасностью
образов

Сетевая безопасность

Анализ прав доступа

Защита Runtime

Обновления в Luntry 4.6

Контроль
Kubernetes-ресурсов

Контроль состояния Kubernetes-
кластеров

Контроль соответствия кластера
стандартам



Управление безопасностью
образов

Сетевая безопасность

Анализ прав доступа

Защита Runtime

LUNTRY 4.6

	LUNTRY 4.6
Модуль Runtime защиты	• Добавление Host Runtime Rules • Добавление Prevention Policies • Добавление поддержки не оркестрируемых окружений Docker Rules
Модуль сетевой безопасности	• Генерация DNS политик для CNI Cilium
Модуль безопасности образов	• Новые виды отчетов • Продвинутая приоритезация найденных уязвимостей с учетом различных факторов • Добавление поддержки Threat Intelligence (TI) от Solar 4Rays



PREVENTION POLICIES

Задача для runtime

- Исключить запуск нежелательных исполняемых файлов внутри контейнера
 - Подход через whitelist и blacklist

The screenshot displays the 'Prevention Policies' management interface. At the top, there are tabs for 'Runtime Policies', 'Policy Engines', 'Runtime Rules', 'Prevention Policies', 'Host Runtime Rules', 'Reaction Policies', 'Security Gates', and 'Audit Rules'. The 'Prevention Policies' tab is active, showing a table of policies. Below the table, there is a modal form for editing a policy.

Name	Description	Policy Type	Namespace	Container	Parent Name	Parent Kind	Alerts Count	Updated At
block du	block du	Block	default	dnsutils	dnsutils	Pod	0	10.08.2026 15:34:50

Policy Details Form:

- Name:** block du
- Description:** block du
- Namespace:** default
- Container Name:** dnsutils
- High Level Parent Kind:** Pod
- High Level Parent Name:** dnsutils
- Allow Rules:** [Add new allow rules](#)
- Audit Rules:** [Add new audit rules](#)
- Block Rules:** Parent commands separated by commas
[Add new block rules](#) [Delete all block rules](#)

[Save](#) [Cancel](#)



HOST RUNTIME RULES

LUNTRY

- 11

Host Runtime Rules > Detects

Runtime Policies | Policy Engines | Runtime Rules | Prevention Policies | Host Runtime Rules | Docker Rules | Reaction Policies | Security Gates | Audit Rules

Dashboard **Rules** **Detects**

Search... 02.09.2026 00:00 - 02.09.2026 20:54 Type 3

Time	Rule	Type	Cluster	Hostname
02.09.2026 17:21:45	Write /etc/passwd	file	main	gimme-f0b17739-2
02.09.2026 17:50:53	Write /etc/passwd	file	main	gimme-f0b17739-2
02.09.2026 17:33:53	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:53	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:53	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:53	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:53	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:53	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:53	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:53	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:54	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:54	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:54	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:54	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:58	Detect apt-get	process	main	gimme-f0b17739-2
02.09.2026 17:33:58	Detect apt-get	process	main	gimme-f0b17739-2

Items per page: 25 1 - 25 of 44 < >

Name: Write /etc/passwd

Type: File

Date: 02.09.2026 17:21:45 (about 6 hours ago)

Node: gimme-f0b17739-2

Cluster: main

Process exepaths: /usr/lib/systemd/systemd
/usr/sbin/sshd
/usr/sbin/sshd
/usr/bin/bash
/usr/bin/nano

Detect Info:

GID: 0

PID: 26587

PPID: 25876

Command: nano

Arguments: /etc/passwd

Path: /etc/passwd

Mode: FILEACCESSMODE_WRONLY

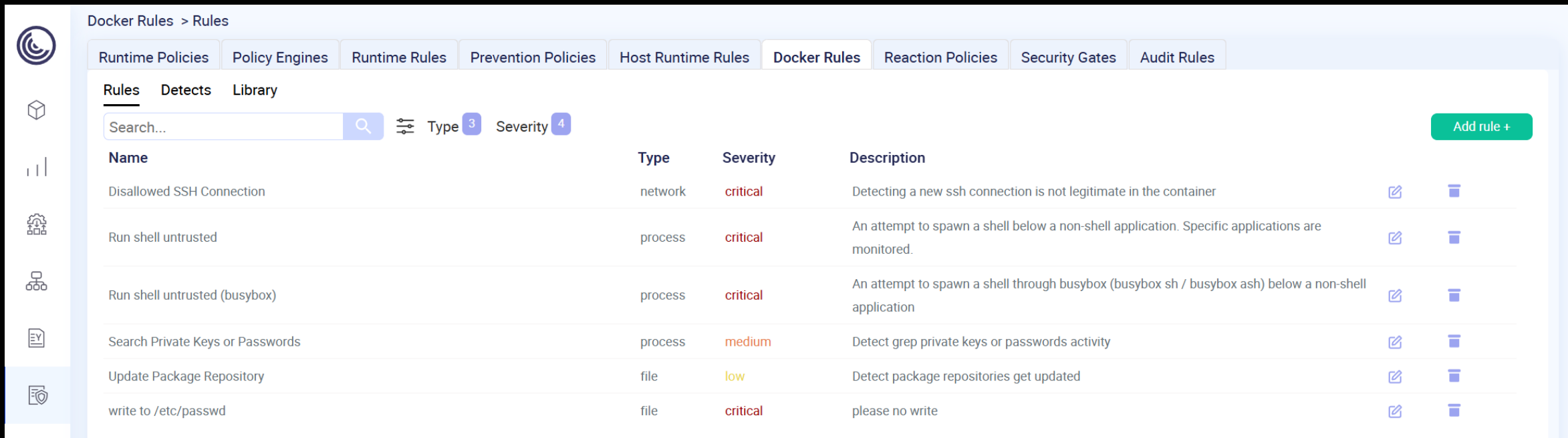


DOCKER RULES

НЕОРКЕСТРИРУЕМЫЕ ОКРУЖЕНИЯ

Задача для runtime

- Обнаружить вредоносную, нежелательную активность в контейнере в не оркестрируемом окружении
 - Аналог Runtime Rules, но для Docker, Podman
 - Атакующий внутри Docker контейнера



The screenshot displays the 'Docker Rules > Rules' interface. It features a navigation bar with tabs: Runtime Policies, Policy Engines, Runtime Rules, Prevention Policies, Host Runtime Rules, Docker Rules (selected), Reaction Policies, Security Gates, and Audit Rules. Below the tabs, there are sub-tabs: Rules, Detects, and Library. A search bar and filters for Type (3) and Severity (4) are present. A table lists several rules, each with a Name, Type, Severity, and Description. Action icons (edit and delete) are visible for each rule.

Name	Type	Severity	Description
Disallowed SSH Connection	network	critical	Detecting a new ssh connection is not legitimate in the container
Run shell untrusted	process	critical	An attempt to spawn a shell below a non-shell application. Specific applications are monitored.
Run shell untrusted (busybox)	process	critical	An attempt to spawn a shell through busybox (busybox sh / busybox ash) below a non-shell application
Search Private Keys or Passwords	process	medium	Detect grep private keys or passwords activity
Update Package Repository	file	low	Detect package repositories get updated
write to /etc/passwd	file	critical	please no write



ГЕНЕРАЦИЯ DNS ПОЛИТИК ДЛЯ CNI CILUM

Задача сетевой безопасности

- Гранулированной сетевой контроль исходящего трафика из кластера
- Решение проблемы динамических IP
- Микросегментация для внешних зависимостей

```
apiVersion: cilium.io/v2
kind: CiliumNetworkPolicy
metadata:
  creationTimestamp: null
  name: luntry-np-pod-default-curl-loop-5
  namespace: default
spec:
  egress:
    - toCIDR:
        - 156.137.3.32/32
      toPorts:
        - ports:
            - port: "443"
              protocol: TCP
    - toFQDNs:
        - matchName: dhl.com.
        - matchName: fedex.com.
        - matchName: www.dhl.com.
        - matchName: express.dhl.ru.
        - matchName: www.fedex.com.
        - matchName: www.logistics.dhl.ru.
```



НОВАЯ THREAT INTELLIGENCE (TI) ИНФОРМАЦИЯ

Задача анализа образов

- Анализ ОС базового слоя образа
 - Контроль в Security Gates
- Анализ EOL (End Of Live) программных продуктов и пакетов
 - Новый тип отчета
 - Контроль в Security Gates
- Анализ на вредоносные пакеты (Malicious packages)
 - Новый тип отчета
 - Контроль в Security Gates
- Поддержка YARA-правил от Solar 4Rays для обнаружения malware
 - Уникальная экспертиза и детекты



СТЕМ

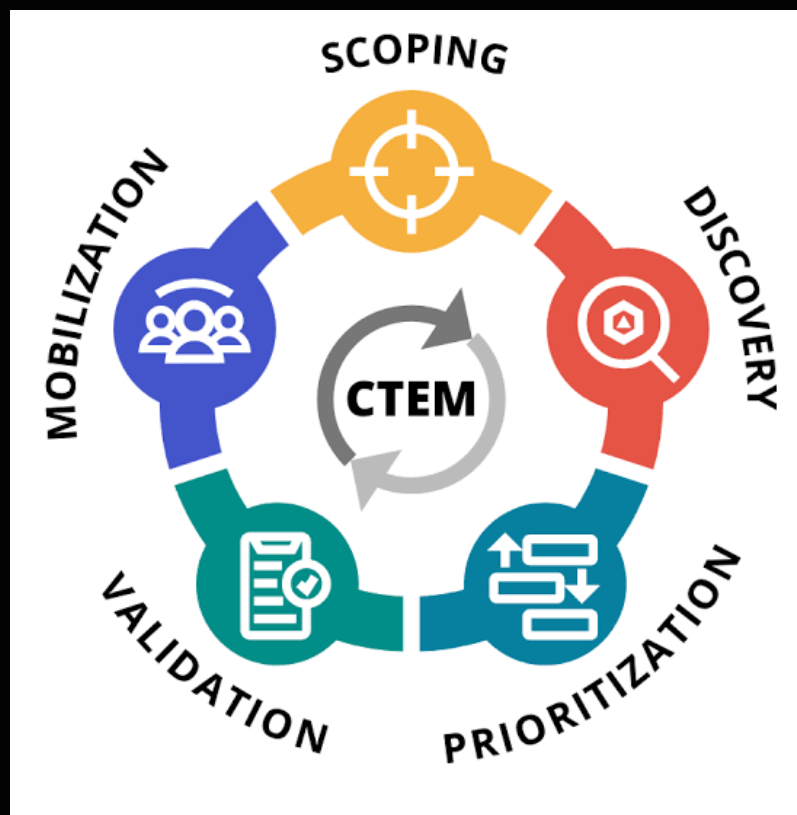
**ПРОДВИНУТАЯ ПРИОРИТЕЗАЦИЯ НАЙДЕННЫХ
УЯЗВИМОСТЕЙ**

Задача по работе с уязвимостями

- Уязвимостей много
 - Даже с уровнем критичности Critical и High
 - Невозможно окружение без уязвимостей вообще
- Уязвимости постоянно появляются
 - Время играет против нас
 - Преимущество на стороне атакующего
- Исправления требуют вовлечение/отвлечение специалистов
 - Страдает развитие продукта
 - Специалистов не хватает

Что такое STEM?

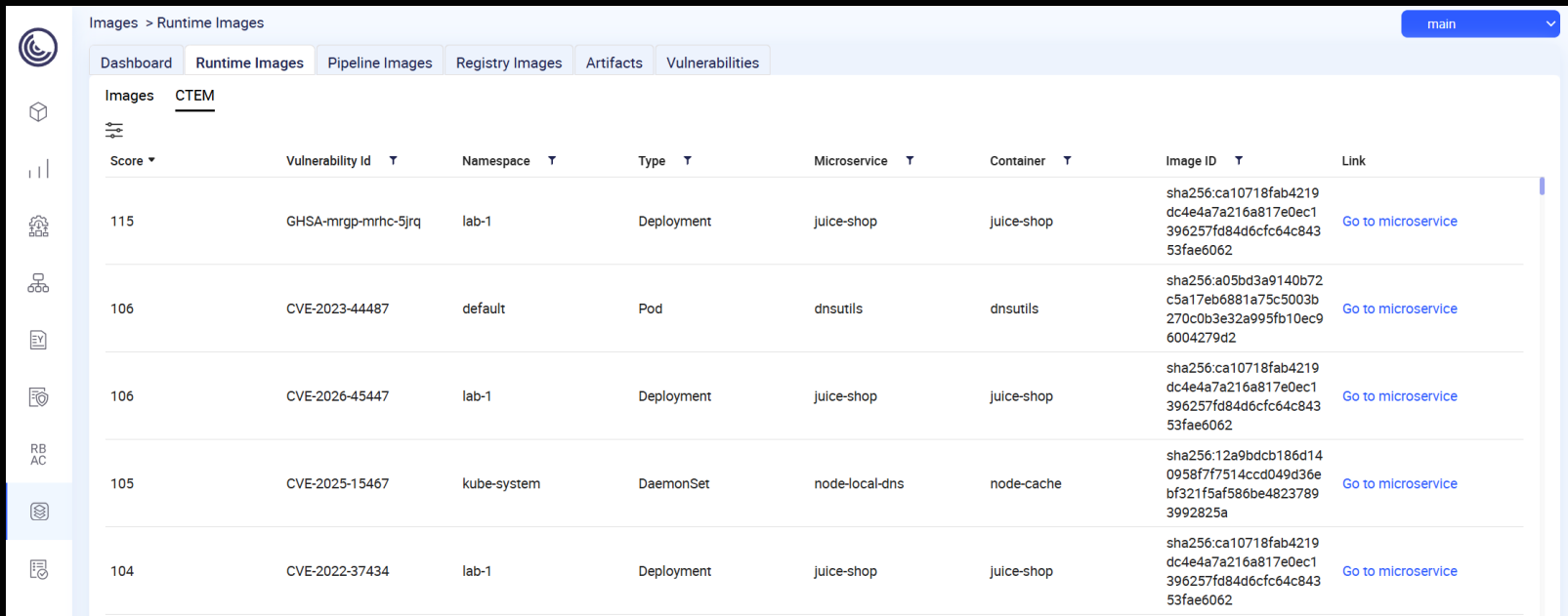
- STEM (Continuous Threat Exposure Management) в информационной безопасности — это проактивная методология непрерывного выявления, оценки, приоритизации и устранения киберугроз и уязвимостей в цифровых активах компании.



STEM в LUNTRY

Для приоритезации уязвимостей в образах контейнеров учитывается информация о:

- Уязвимости
- Эксплоитах и атаках
- Свойства контейнера
- Сетевом расположении и доступности
- Примененных мер безопасности к микросервису



Images > Runtime Images							
main							
Dashboard Runtime Images Pipeline Images Registry Images Artifacts Vulnerabilities							
Images CTEM							
Score	Vulnerability Id	Namespace	Type	Microservice	Container	Image ID	Link
115	GHSA-mrgp-mrhc-5jrq	lab-1	Deployment	juice-shop	juice-shop	sha256:ca10718fab4219dc4e4a7a216a817e0ec1396257fd84d6cfc64c84353fae6062	Go to microservice
106	CVE-2023-44487	default	Pod	dnsutils	dnsutils	sha256:a05bd3a9140b72c5a17eb6881a75c5003b270c0b3e32a995fb10ec96004279d2	Go to microservice
106	CVE-2026-45447	lab-1	Deployment	juice-shop	juice-shop	sha256:ca10718fab4219dc4e4a7a216a817e0ec1396257fd84d6cfc64c84353fae6062	Go to microservice
105	CVE-2025-15467	kube-system	DaemonSet	node-local-dns	node-cache	sha256:12a9bdc186d140958f7f7514ccd049d36ebf321f5af586be48237893992825a	Go to microservice
104	CVE-2022-37434	lab-1	Deployment	juice-shop	juice-shop	sha256:ca10718fab4219dc4e4a7a216a817e0ec1396257fd84d6cfc64c84353fae6062	Go to microservice



ROADMAP LUNTRY

RoadMap Luntry

	Luntry 5.0
Модуль Runtime защиты	• Реализация функциональности SOAR
Модуль сетевой безопасности	• Конструктор NetworkPolicy
Модуль безопасности образов	• Пользовательские правила на YARA
Модуль контроля Kubernetes-ресурсов	• Обновление библиотеки детектов для Kubernetes Audit Log • Обновление библиотеки политик для PolicyEngines (VAP)
Модуль состояния Kubernetes-кластеров	• Анализ безопасности хостовой ОС
Общее	• Выпуск обновленного UI/UX • Продвинутое предоставление прав доступа и области видимости пользователей • Обработка 1M EPS

5.0

UX/UI

Images / cr.yandex/crpsjg1coh47p81vh2lc/k8s-addons/calico/cluster-proportional-autoscaler-amd64

Cluster: Main

Hi Batman

Image

cr.yandex/crpsjg1coh47p81vh2lc/k8s-addons/calico/cluster-pro...

sha256:66508f57eb6542a3bfabfd60b41828522071a6ac1a59c9a2a464339d8e50e5c8

745

Download in XML

APIgroup: rbac.authorization.k8s.io

Version: rbac.authorization.k8s.io

19:15 29.08.2024

Data

docker.io bitnami kubect:l:1.28.5

Summary

Severity ☒ critical ☒ high ☒ medium ☒ low ☒ info

Fix state ☒ fixable ☒ unfixable

66 1950 156 1583 714

View: Vulnerabilities

CVE 517 Secrets 517 Config 2 Vulnerabilities 517

Layers SBOM

Search

Search area: Components

Filters

Sorting

CVSS AV:N

CVE-2023-45853 3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

☒ ☒

RCE

0.71629

fixed ☒

▼

KEV: 11.07.2024

Exploit: rbac.authorization.k8s.io

Links: <http://www.openwall.com/lists/oss-security/20...>
<https://my.f5.com/manage/s/article/K000138445>
<http://www.openwall.com/lists/oss-security/20...>

Description:

When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module, undisclosed requests can cause NGINX worker processes to terminate. Note: The HTTP/3 QUIC module is not enabled by default and is considered experimental. For more information, refer to Support for QUIC and HTTP/3 <https://nginx.org/en/docs/quic.html>.
Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

CVE-2023-45853 3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

☒ ☒

RCE

0.71629

fixed ☒

▼

5.0

UX/UI

cluster: Main

Images

Hi Batman

Images

Download in XML

Summary

Severity

☒ critical

☒ high

☒ medium

☐ low

☒ info

Fix state

☒ fixable

☒ unfixable

66

1950

1583

714

156

View: Images

Runtime 517

Secrets 517

Config 2

Search

Search area: Components

Filters

Sorting

CVSS AV:N

CVSS AV:N

CVSS AV:N

component	alpine-baselayout-data		2		1		5	9	9	9	9	9	9	2/4	
component	alpine-baselayout-data		2		1		5	9	9	9	9	9	9	2/4	
component	alpine-baselayout-data		2		1		5	9	9	9	9	9	9	2/4	
component	alpine-baselayout-data		2		1		5	9	9	9	9	9	9	2/4	
component	alpine-baselayout-data		2		1		5	9	9	9	9	9	9	2/4	
component	alpine-baselayout-data		2		1		5	9	9	9	9	9	9	2/4	



📍 [luntry_official](#)

📍 [luntrysolution](#)

📍 [luntrysolution](#)

🌐 [luntry.ru](#)

✉ [info@luntry.ru](#)

ДМИТРИЙ ЕВДОКИМОВ
Founder & CTO Luntry

✉ [de@luntry.ru](#)

📍 [Qu3b3c](#)

📍 [k8security](#)

**СПАСИБО
ЗА ВНИМАНИЕ!**