Оглавление

[CVE-2023-44487 2](#_Toc172193039)

[Описание 2](#_Toc172193040)

[Шаги по снижению риска атак, первый источник 2](#_Toc172193041)

[Второй источник 2](#_Toc172193042)

[Хосты 3](#_Toc172193043)

[Виртуальные машины 3](#_Toc172193044)

[Образы 4](#_Toc172193045)

[CVE-2021-44228 9](#_Toc172193046)

[Описание 9](#_Toc172193047)

[Что можно сделать для защиты 9](#_Toc172193048)

[Хосты: 9](#_Toc172193049)

[Образы: 9](#_Toc172193050)

[CVE-2023-4863 10](#_Toc172193051)

[Описание 10](#_Toc172193052)

[Рекомендации: 10](#_Toc172193053)

[Хосты 10](#_Toc172193054)

[Виртуальные машины 10](#_Toc172193055)

[Образы 10](#_Toc172193056)

[**CVE-2023-4911** 12](#_Toc172193057)

[Описание 12](#_Toc172193058)

[Смягчение 12](#_Toc172193059)

[Хосты: 13](#_Toc172193060)

[Образы 13](#_Toc172193061)

[**CVE-2024-1086** 16](#_Toc172193062)

[Описание 16](#_Toc172193063)

[Смягчение 16](#_Toc172193064)

[Хосты: 16](#_Toc172193065)

[Виртуальные машины 16](#_Toc172193066)

# CVE-2023-44487

## Описание

Обнаружена уязвимость в обработке мультиплексированных потоков в протоколе HTTP/2. Клиент может многократно делать запрос на новый мультиплексный поток и немедленно отправлять кадр RST\_STREAM для его отмены. Это создает дополнительную работу для сервера по настройке и разрыву потоков, не достигая при этом какого-либо серверного ограничения на максимальное количество активных потоков на соединение, что приводит к отказу в обслуживании из-за потребления ресурсов сервера. Red Hat оценила серьезность этой уязвимости как «важную», поскольку Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) объявило эту уязвимость активным эксплойтом.

Уязвимость CVE-2023-39325 была назначена для атаки Rapid Reset в языковых пакетах Go.

## Шаги по снижению риска атак, первый источник

Будучи полнофункциональным сервером и прокси-сервером, NGINX предоставляет администраторам мощные инструменты для предотвращения атак типа «отказ в обслуживании». Чтобы воспользоваться этими функциями, важно внести следующие обновления в файлы конфигурации NGINX, чтобы минимизировать поверхность атаки сервера:

* Для параметра [keepalive\_requests](https://nginx.org/en/docs/http/ngx_http_core_module.html" \l "keepalive_requests" \t "_blank) следует оставить значение по умолчанию - 1000 запросов.
* Для [http2\_max\_concurrent\_streams](https://nginx.org/en/docs/http/ngx_http_v2_module.html#http2_max_concurrent_streams) следует оставить значение по умолчанию - 128 потоков.

Также рекомендуется добавить следующие меры безопасности в качестве передовой практики:

* [limit\_conn](https://nginx.org/en/docs/http/ngx_http_limit_conn_module.html) устанавливает ограничение на количество разрешенных подключений от одного клиента. Эту директиву следует добавить с разумной настройкой, обеспечивающей баланс между производительностью и безопасностью приложения.
* [limit\_req](https://nginx.org/en/docs/http/ngx_http_limit_req_module.html) устанавливает ограничение на количество запросов, которые будут обработаны в течение заданного периода времени от одного клиента. Эту директиву следует добавить с разумной настройкой, обеспечивающей баланс между производительностью и безопасностью приложения.

Чтобы обеспечить раннее обнаружение флуд-атак команда NGINX выпустила патч, для модуля ngx\_http\_v2\_module, накладывающий ограничение на количество новых потоков, которые могут быть введены в один цикл событий. Этот предел устанавливается в два раза больше значения, настроенного с помощью директивы http2\_max\_concurrent\_streams. Ограничение будет применено, даже если максимальный порог никогда не будет достигнут, например, когда потоки сбрасываются сразу после отправки запроса (как в случае с этой атакой).

## Второй источник

Пользователям настоятельно рекомендуется обновить свое программное обеспечение, как только появятся исправления.

Существует несколько подходов к устранению этой уязвимости.

1. Если позволяют обстоятельства, пользователи могут отключить конечные точки http2, чтобы полностью обойти уязвимость, пока не будет доступно исправление.

2. Блокировка на основе IP или защита от флуда и инструменты управления скоростью могут использоваться на конечных точках сети для фильтрации входящего трафика.

3. Также доступно несколько мер по смягчению последствий для конкретных пакетов.

a. nginx: <https://www.nginx.com/blog/http-2-rapid-reset-attack-impacting-f5-nginx-products/>

b. netty: <https://github.com/netty/netty/security/advisories/GHSA-xpw8-rcwv-8f8p>

c. haproxy: <https://www.haproxy.com/blog/haproxy-is-not-affected-by-the-http-2-rapid-reset-attack-cve-2023-44487>

d. nghttp2: <https://github.com/nghttp2/nghttp2/security/advisories/GHSA-vx74-f528-fxqg>

e. golang: ограничение потокового параллелизма по умолчанию в golang составляет 250 потоков (запросов) на соединение HTTP/2. Это значение можно настроить в пакете golang.org/x/net/http2 с помощью настройки Server.MaxConcurrentStreams и функции ConfigureServer, которые доступны в golang.org/x/net/http2.

## Хосты

### Виртуальные машины

|  |
| --- |
|  |
| **Имя ресурса** | **Аккаунт** | **ID аккаунта** | **Публично доступен** | **Высокие привилегии** | **Регион** |  |  |
| sbc-k8s-infra-prod-0 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | Да | - | RU-Moscow |  |  |
| sbc-k8s-infra-0-stage1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | Да | - | RU-Moscow |  |  |
| sbc-k8s-infra-prod-2 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | Да | - | RU-Moscow |  |  |
| ecs-ds-rpa-gitrunner | ru-moscow-1\_ATD-services | 1132b4e37f0024f22f9fc01742c2cdf2 | Да | - | RU-Moscow |  |  |
| ecs-linux-runner | ru-moscow-1\_JavaMiddle | 10745f2d440027312f7bc017a5f63010 | Да | - | RU-Moscow |  |  |
| ecs-DA | ru-moscow-1\_DA | 102432e2500025e42fe7c0171744fbfe | Да | - | RU-Moscow |  |  |
| sbc-k8s-worker-prod2 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-worker-0-stage1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-infra-prod-1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-worker-1-stage1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-worker-prod1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-worker-prod0 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| nexus | ru-moscow-1\_RHOS | 10196eb6b28026e02fddc017d18726ab | - | - | RU-Moscow |  |  |
| sbc-jenkins-01 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| nexus | ru-moscow-1\_OpenShift | 1026bfce990026e02f64c0172ee8b343 | - | - | RU-Moscow |  |  |

### Образы

| **Имя ресурса** | **Namespace** | **Кластер** | **Репозиторий** | **SHA256** | **Количество** |
| --- | --- | --- | --- | --- | --- |
| everest-csi-driver-init:2.1.30 | 1 | 1 | swr.ru-moscow-1.hc.sbercloud.ru/hwofficial | 0277f5aef660753e1bcfe9d737025c1b845ba70244511e3d79d66bdad45dcbaa | 1 |
| jaeger-collector:1.49.0 | 1 | 2 | jaegertracing | 06ee1b5882dfb55db6c5393c0a88455b20ae97a382e7cdc1a24a118dc9555108 | 1 |
| jaeger-query:1.49.0 | 1 | 1 | jaegertracing | 03ac133f70fca773a8adc4c4df2dc9dbdabaee5cb15c19fd6a75c8590ac39f1f | 1 |
| jaeger-operator:1.49.0 | 1 | 2 | jaegertracing | 05a09105372446c53bd285ae1fbbdc9f78723a6089bebac85f4194e0ee6b19ab | 1 |
| vault-k8s:0.14.1 | 1 | 2 | hashicorp | 0c61baa9a7e2206f89604df93e904f96158be02d7e2be295695c91707ebcd022 | 1 |
| redis-operator:v0.11.0 | 1 | 1 | quay.io/opstree | 1572cbc8edebba6b2fa387ccc8d11e69932e4622b09de082fc4b4d793969b198 | 1 |
| eduterm-landing:release-2.13.0 | 1 | 2 | sbc-nexus-01.sbc.local:5002 | 270394f4ec6303bc23257b10fc9d091ddb8d99924f5b9ce6addf921b9028b60b | 1 |
| eduterm-ui:wqm1 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 48923a80525dd5252301d7d3eebd5685eca830d42f0743f04081f335c6fc7f74 | 1 |
| eduterm-ui:release-2.13.0 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 7a208f07d84d0d46406aaf51054a3fe6f730e321beed4043380e616947452d44 | 1 |
| eduterm-admin-front:release-2.13.0 | 1 | 2 | sbc-nexus-01.sbc.local:5002 | f28f969772312e44f0f0994636f2b4c360450b77941dd200f27f8b19b28f23c3 | 1 |
| grafana:10.1.2 | 1 | 1 | grafana | 31656ec60d2e7c17b994d38d32f41aa13221cd2aa6d9cb6c2af521fb54ccd60d | 1 |
| jaeger-query:1.39.0 | 1 | 1 | jaegertracing | 3ea5a9b9bd350df635c3aa9f1d08888053c379f7b67d986f63218ba5c0d92b1c | 1 |
| cert-manager-controller:v1.13.1 | 1 | 2 | quay.io/jetstack | 3272e1b8b13ba0c89fc229a213968da386ade046b48cbb6da559c068c9864c0a | 1 |
| eck-operator:2.3.0 | 1 | 2 | sbc-nexus-01.sbc.local:5000/elastic | 3ece38a5265d73222b25a70f45a1ab88ce3e2f8846fb5280d505839ae0d22f09 | 1 |
| metrics-exporter:0.21.3 | 1 | 1 | altinity | 3f9380b13393828fb3d947b1f157348fb12238370db9b4c3b9d8f29e3f41f002 | 1 |
| clickhouse-operator:0.21.3 | 1 | 1 | altinity | 46e0e4ac901a6129cfe19e28a8dea042862b0a4bb89de3793d9bfa54151f6350 | 1 |
| node-exporter:v1.6.1 | 1 | 1 | quay.io/prometheus | 458e026e6aa62a8da4522cb09766da69d7365ebeb456d5a43a214fc6bd232a3c | 1 |
| coredns:1.25.11 | 1 | 1 | swr.ru-moscow-1.hc.sbercloud.ru/hwofficial | 5c3ecfbc8a13b57232c7953a34a69150ff3d350bf27792133119fb7ac7dc3f81 | 1 |
| coredns:1.27.4 | 1 | 1 | swr.ru-moscow-1.hc.sbercloud.ru/hwofficial | 81717b52301fa856d91aabd1441075ff1059ca738c28d0aced61883d7de58a69 | 1 |
| icagent:5.12.139 | 1 | 2 | swr.ru-moscow-1.hc.sbercloud.ru/op\_svc\_apm | 5e0671aaa748c4abbfb0ef5211b4686356302091a0e216c6b6bc974a164c2f12 | 1 |
| kibana:7.14.0 | 1 | 2 | sbc-nexus-01.sbc.local:5000/elasticsearch | 58dffcbc8caa43c7bb0084fb51b29706bc0dca39405b39b67f4923988b11c527 | 1 |
| ubi-minimal:latest | 1 | 1 | registry.access.redhat.com/ubi8 | 875fa650d56e4c4750089ffbe1de555af2627c33c9f585cf1bbd33e100601cf2 | 1 |
| elasticsearch:7.14.0 | 2 | 2 | sbc-nexus-01.sbc.local:5000/elasticsearch | e347b2b2d6c139e00250755db2a77c993176bdbbc5daecc5c0c3a3b04004b186 | 1 |
| jaeger-ingester:1.49.0 | 1 | 2 | jaegertracing | 6f066ef323ec21d966a3c1b25a476db1f3219c5c04501a5b40a29026a70bfa0a | 1 |
| everest:2.1.30 | 1 | 1 | swr.ru-moscow-1.hc.sbercloud.ru/hwofficial | 6f4a5b4a5c6c3c6f5554fbf97203ac6e31b0c23719611e60d7fd2185d54d1370 | 1 |
| everest:2.1.51 | 1 | 1 | swr.ru-moscow-1.hc.sbercloud.ru/hwofficial | e532776f149e5dedf3b766147624f08e7afc0642316b7165f14cb92b46930115 | 1 |
| proxyv2:1.18.3 | 2 | 2 | istio | 7480ba3d459aa923093ac9c913cb95672737a068ca06e8144cd65af952820f46 | 1 |
| pilot:1.18.3 | 1 | 2 | istio | fbd935fc526ecfd88287bcf576e81e21919d00dfc69e80017ce851217d6a6fc7 | 1 |
| operator:1.18.3 | 1 | 2 | istio | fc7ad03c947fc9567c96fcc39a428424ab5ca1e6f97ad0af2c6d19f3d695960a | 1 |
| jaeger-agent:1.39.0 | 1 | 1 | jaegertracing | 79b56e14f0a4540f0e81e2a7589be2845a76ff0fae877aceb8fa9a3b583eb724 | 1 |
| everest-csi-driver-init:2.1.51 | 1 | 1 | swr.ru-moscow-1.hc.sbercloud.ru/hwofficial | 7d51d0cfa9178bcf90cec0e6e70703ce0fe9d5706b0d034708576b2c2f0d80c8 | 1 |
| prometheus-operator:v0.68.0 | 1 | 1 | quay.io/prometheus-operator | 833596d498b13aa749e2745c6d4af1888b22c5517a3f8f460d1907fd774ed67a | 1 |
| jaeger-agent:1.49.0 | 1 | 1 | jaegertracing | 82cbe0bab645ab65fda28e0f60d78a889433d1422c98d3f21bbe26ae9feef18b | 1 |
| ratelimit:568c537d | 1 | 2 | envoyproxy | 892a84cd552b97c057f507b77decce2b8e109ec28170682263c153865b1a8369 | 1 |
| eduterm-oauth2-proxy:753ed4b35b3 | 1 | 2 | sbc-nexus-01.sbc.local:5002 | 88ba3b9c41729ef66edc6ae5021724cc0a544fc651dcb4cad06e5180b118feac | 1 |
| kube-state-metrics:v2.10.0 | 1 | 1 | registry.k8s.io/kube-state-metrics | 8e0f85b91e3b0fb93d7a16af25923f4f46a1dee2e79d1de16e55c2727139198e | 1 |
| prometheus:v2.42.0 | 1 | 2 | quay.io/prometheus | 8cfcb66f43649bbe426a25511440c645018b9cf5ddcf05aacef582a052ad474b | 1 |
| vault:1.9.0 | 2 | 1 | hashicorp | 996ebb03026415698fac1785c57672eb40c0a6e7f8138233815046c3f3511e58 | 1 |
| vault:latest | 3 | 2 | valex1984 | ef2b782aa5effa9dfe7717f512c3c775799d8c79536f8b0288c4235882736634 | 1 |
| cert-manager-webhook:v1.13.1 | 1 | 2 | quay.io/jetstack | c172f69eb03e128c2a5d8a68a6fb8fbe70c6822fcb2944998c1fba071172b429 | 1 |
| alertmanager:v0.25.0 | 1 | 2 | quay.io/prometheus | c8568f914cd25b2062c44e9f79f9c18da6e3b85fe0c47a12a2191c61426c2b19 | 1 |
| cert-manager-cainjector:v1.13.1 | 1 | 2 | quay.io/jetstack | cd3c430bf95243c7a3bb86b9c75496d0125eab339735fcc6d38050bd19f49328 | 1 |
| curl:7.85.0 | 1 | 2 | curlimages | dddbb581f872d3d5a5083a31888badf4aace9bd73a6393d2289f9d47667b92c2 | 1 |
| dex:v2.30.0 | 1 | 2 | harbor-dev.pcbltools.ru/base\_images/dexidp | e30b0e044d4b4fabdc9f7112ea67b023ef6e8827bbca2f3da729f058fa6531f2 | 1 |
| prometheus-config-reloader:v0.68.0 | 1 | 1 | quay.io/prometheus-operator | e91710e6a0f946c839da85ab8d1e57784a880af117bfdd9a3e3bf1a951f420a2 | 1 |

# CVE-2021-44228

## Описание

Apache Log4j2 2.0-beta9 по 2.15.0 (исключая выпуски безопасности 2.12.2, 2.12.3 и 2.3.1) Функции JNDI, используемые в конфигурации, сообщениях журнала и параметрах, не защищают от контролируемых злоумышленником LDAP и других конечных точек, связанных с JNDI. Злоумышленник, который может контролировать сообщения журнала или параметры сообщений журнала, может выполнить произвольный код, загруженный с серверов LDAP, когда включена подстановка поиска сообщений. Начиная с log4j 2.15.0, это поведение отключено по умолчанию. Начиная с версии 2.16.0 (вместе с 2.12.2, 2.12.3 и 2.3.1) эта функциональность полностью удалена. Обратите внимание, что эта уязвимость специфична для log4j-core и не затрагивает log4net, log4cxx или другие проекты Apache Logging Services.

## Что можно сделать для защиты

В первую очередь [обновите](https://logging.apache.org/log4j/2.x/download.html) Apache Log4j до последней версии.

Если по какой-то причине нет возможности обновиться, используйте эти рекомендации.

1. В версиях 2.10 и выше можно установить системное свойство log4j2.formatMsgNoLookups или переменную среды LOG4J\_FORMAT\_MSG\_NO\_LOOKUPS в значениеtrue.
2. В версиях с 2.7 до 2.14.1 можно изменить шаблоны PatternLayout: указать конвертер сообщений как %m{nolookups} вместо простого %m.
3. В 2.0-beta9 до 2.7 единственный возможный вариант — полностью удалить JndiLookup из маршрута к классам: zip q -d log4j-core\*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class.

## Хосты:

### Образы:

| **Имя ресурса** | **Namespace** | **Кластер** | **Репозиторий** | **SHA256** | **Количество** |
| --- | --- | --- | --- | --- | --- |
| elasticsearch:7.14.0 | 2 | 2 | sbc-nexus-01.sbc.local:5000/elasticsearch | e347b2b2d6c139e00250755db2a77c993176bdbbc5daecc5c0c3a3b04004b186 | 1 |

# CVE-2023-4863

## Описание

CVE-2023-4863 – уязвимость, связанная с переполнением буфера во время работы с WebP (формат изображения, созданный Google). Этот формат, обеспечивающий высокое качество сжатия изображений, активно применяется в интернете. В случае открытия специально сформированной картинки в формате WebP злоумышленник может выполнить вредоносный код в системе с правами пользователя, запустившего приложение

## Рекомендации:

1. установить с сайта производителя последнюю версию ПО (Chrome, Safari, Opera, Edge, Firefox, Thunderbird и т.п.);
2. до обновления браузера можно отключить в нем функционал обработки изображений в формате WebP:
   * Chrome:
     1. - в адресной строке ввести chrome://flags;
     2. в поиске ввести WebP;
     3. выключить Lens Optimized Image Formats;
   * Firefox:
     1. - в адресной строке ввести about:config;
     2. - в поиске ввести WebP;
     3. - отключить image.webp.enabled
3. при использовании продукта UserGate NGFW можно создать правило контентной фильтрации, запрещающее Content-Type "image/webp" (необходима настройка дешифровки пользовательского трафика в SSL Inspection).

## Хосты

### Виртуальные машины

| **Имя ресурса** | **Аккаунт** | **ID аккаунта** | **Публично доступен** | **Высокие привилегии** | **Регион** |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| nexus | ru-moscow-1\_RHOS | 10196eb6b28026e02fddc017d18726ab | - | - | RU-Moscow |  |  |

### Образы

| **Имя ресурса** | **Namespace** | **Кластер** | **Репозиторий** | **SHA256** | **Количество** |
| --- | --- | --- | --- | --- | --- |
| eduterm-landing:release-2.13.0 | 1 | 2 | sbc-nexus-01.sbc.local:5002 | 270394f4ec6303bc23257b10fc9d091ddb8d99924f5b9ce6addf921b9028b60b | 1 |
| eduterm-ui:wqm1 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 48923a80525dd5252301d7d3eebd5685eca830d42f0743f04081f335c6fc7f74 | 1 |
| eduterm-ui:release-2.13.0 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 7a208f07d84d0d46406aaf51054a3fe6f730e321beed4043380e616947452d44 | 1 |
| eduterm-admin-front:release-2.13.0 | 1 | 2 | sbc-nexus-01.sbc.local:5002 | f28f969772312e44f0f0994636f2b4c360450b77941dd200f27f8b19b28f23c3 | 1 |

# **CVE-2023-4911**

## Описание

Переполнение буфера было обнаружено в динамическом загрузчике ld.so библиотеки GNU C при обработке переменной среды GLIBC\_TUNABLES. Эта проблема может позволить локальному злоумышленнику использовать вредоносные переменные среды GLIBC\_TUNABLES при запуске двоичных файлов с разрешением SUID для выполнения кода с повышенными привилегиями.

Смягчение

Для клиентов, которые не могут выполнить обновление немедленно и не включили функцию Secure Boot, проблему можно устранить с помощью предоставленного скрипта SystemTap, выполнив следующие шаги. При включении любая программа setuid, вызванная с помощью GLIBC\_TUNABLES в среде, будет немедленно завершена. Чтобы вызвать программу setuid, пользователям придется сбросить или очистить переменную окружения GLIBC\_TUNABLES, например, `GLIBC\_TUNABLES= sudo` .

Обратите внимание, что эти шаги по смягчению последствий придется повторить в случае перезагрузки системы.

1) Установите необходимые пакеты systemtap и зависимости согласно - <https://access.redhat.com/solutions/5441>

2) Создайте следующий скрипт systemtap и назовите его stap\_block\_suid\_tunables.stp:

function has\_tunable\_string:long()   
{   
 name = "GLIBC\_TUNABLES"   
  
 mm = @task(task\_current())->mm;   
 if (mm)   
 {   
 env\_start = @mm(mm)->env\_start;   
 env\_end = @mm(mm)->env\_end;   
  
 if (env\_start != 0 && env\_end != 0)   
 while (env\_end > env\_start)   
 {   
 cur = user\_string(env\_start, "");   
 env\_name = tokenize(cur, "=");   
   
 if (env\_name == name && tokenize("", "") != "")   
 return 1;   
 env\_start += strlen (cur) + 1   
 }   
 }   
  
 return 0;   
}   
  
probe process("/lib\*/ld\*.so\*").function("\_\_tunables\_init")   
{   
 atsecure = 0;   
 /\* Пропустить обработку, если мы не можем прочитать \_\_libc\_enable\_secure, например,   
 обработчик дампа ядра (systemd-cgroups-agent и systemd-coredump). \*/   
 try { atsecure = @var("\_\_libc\_enable\_secure"); }   
 catch { printk (4, sprintf ("CVE-2023-4911: Пропущена проверка: %s (%d)", execname(), pid())); }   
 if (atsecure && has\_tunable\_string ())   
 raise (9);   
}

3) Загрузите модуль systemtap в работающее ядро:

stap -g -F -m stap\_block\_suid\_tunables stap\_block\_suid\_tunables.stp

4) Убедитесь, что модуль загружен:

lsmod | grep -i stap\_block\_suid\_tunables   
stap\_block\_suid\_tunables 249856 0

5) После обновления пакета glibc до версии, содержащей исправление, модуль ядра, сгенерированный systemtap, можно удалить, выполнив:

rmmod stap\_block\_suid\_tunables

Если в системе включена функция Secure Boot, модуль SystemTap должен быть подписан. Для подписи сгенерированного модуля ядра с помощью ключа, зарегистрированного в связке ключей ядра, можно использовать внешний сервер компиляции, или, начиная с SystemTap 4.7, можно подписать модуль без сервера компиляции. Дополнительную информацию см. здесь - <https://www.redhat.com/sysadmin/secure-boot-systemtap>

## Хосты:

### Образы

| **Имя ресурса** | **Namespace** | **Кластер** | **Репозиторий** | **SHA256** | **Количество** |
| --- | --- | --- | --- | --- | --- |
| eduterm-xapi-adapter:release-2.12.1 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 2422641d8f6ca9a065f1c8bcbd13f725f6d143ca1ca6a94662673881213d4e52 | 1 |
| eduterm-assignment:release-2.12.1 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 25dd394d4737826dca0b7f861bf1ca59c46bb095b9c6f32900fe9a6075f2c02c | 1 |
| eduterm-api-access:release-2.13.0 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 2a848d1728abfc9b10490fecf6438a3b774183dcd1753ea1114646384f641251 | 1 |
| eduterm-vmpool:release-2.12.1 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 2e7ec1b762803afd93a2c639422a2e39ddc300bb4afcdb4121706e7fbc9f461e | 1 |
| eduterm-om:release-2.13.0 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 6876bb4945049197e5ae57fd1812cd57f216869d5e336b2d0c4b6d6f674d8b24 | 1 |
| eduterm-portmapper:release-2.12.1 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 6a62012a931fe23c853f37803cfb4cb2e888d0f8b0de1d077302752db70898c5 | 1 |
| eduterm-user:release-2.12.1 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 6c916e3c4a54f486822ee59a18c7b7100bfa26b3b7bee56ca0e7a54cf0a27665 | 1 |
| eduterm-csi:release-2.13.0 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 7e0ed8727ca6881e17e11a8331e44878abffe4e29023d3b681564fd5d18cdef8 | 1 |
| eduterm-im:release-2.13.0 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | 84a0c9a724e2e991484d6c7a8aa9e18aae4fb55868fb981f990ed5a45cff4b59 | 1 |
| eduterm-scm:release-2.13.0 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | a34068f2f1c368fe8d50557b4ea21810aa0bb631e02737344380280ccdaba5e4 | 1 |
| eduterm-container-manager:release-2.13.0 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | b8ba44d065ebec8b5564012b535bda0b9432999c6ccf71ce260243c6a17cce4e | 1 |
| eduterm-policy:release-2.12.1 | 1 | 1 | sbc-nexus-01.sbc.local:5002 | ef4a9a81e9f89b6e12f59bd403faf75350e8dcd511b8b30df8429238b8ff6dc5 | 1 |
| kibana:7.14.0 | 1 | 2 | sbc-nexus-01.sbc.local:5000/elasticsearch | 58dffcbc8caa43c7bb0084fb51b29706bc0dca39405b39b67f4923988b11c527 | 1 |
| elasticsearch:7.14.0 | 2 | 2 | sbc-nexus-01.sbc.local:5000/elasticsearch | e347b2b2d6c139e00250755db2a77c993176bdbbc5daecc5c0c3a3b04004b186 | 1 |
| proxyv2:1.18.3 | 2 | 2 | istio | 7480ba3d459aa923093ac9c913cb95672737a068ca06e8144cd65af952820f46 | 1 |
| pilot:1.18.3 | 1 | 2 | istio | fbd935fc526ecfd88287bcf576e81e21919d00dfc69e80017ce851217d6a6fc7 | 1 |
| operator:1.18.3 | 1 | 2 | istio | fc7ad03c947fc9567c96fcc39a428424ab5ca1e6f97ad0af2c6d19f3d695960a | 1 |
| ubi-minimal:latest | 1 | 1 | registry.access.redhat.com/ubi8 | 875fa650d56e4c4750089ffbe1de555af2627c33c9f585cf1bbd33e100601cf2 | 1 |

# **CVE-2024-1086**

## Описание

В подсистеме Netfilter в ядре Linux обнаружена уязвимость. Эта проблема возникает в функции nft\_verdict\_init(), допускающей положительные значения как ошибку сброса в вердикте хука, поэтому функция nf\_hook\_slow() может вызвать уязвимость двойного освобождения, когда выдается NF\_DROP с ошибкой сброса, похожей на NF\_ACCEPT. Компонент nf\_tables может быть использован для локального повышения привилегий.

Смягчение

1. Эту уязвимость можно устранить, предотвратив загрузку уязвимого модуля ядра netfilter (nf\_tables). Инструкции по внесению модуля ядра в черный список см. по адресу <https://access.redhat.com/solutions/41278> .

2. Если модуль невозможно отключить, в неконтейнерных развертываниях Red Hat Enterprise Linux решением проблемы является отключение пространств имен пользователей:

# echo "user.max\_user\_namespaces=0" > /etc/sysctl.d/userns.conf   
# sysctl -p /etc/sysctl.d/userns.conf

В контейнерных развертываниях, таких как Red Hat OpenShift Container Platform, не используйте второе смягчение (отключение пространств имен пользователей), так как эта функциональность должна быть включена. Первое смягчение (черный список nf\_tables) по-прежнему применимо для контейнерных развертываний, при условии, что среда не использует netfilter.

## Хосты:

### Виртуальные машины

|  |
| --- |
|  |
| **Имя ресурса** | **Аккаунт** | **ID аккаунта** | **Публично доступен** | **Высокие привилегии** | **Регион** |  |  |
| sbc-k8s-infra-prod-0 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | Да | - | RU-Moscow |  |  |
| sbc-k8s-infra-0-stage1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | Да | - | RU-Moscow |  |  |
| sbc-k8s-infra-prod-2 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | Да | - | RU-Moscow |  |  |
| ecs-29e4 | ru-moscow-1\_student\_lab2 | 10170840900026e02fbbc01795cd7c00 | Да | - | RU-Moscow |  |  |
| ecs-ansible | ru-moscow-1\_ATD-services | 1132b4e37f0024f22f9fc01742c2cdf2 | Да | - | RU-Moscow |  |  |
| ecs-DA | ru-moscow-1\_DA | 102432e2500025e42fe7c0171744fbfe | Да | - | RU-Moscow |  |  |
| ecs-linux-runner | ru-moscow-1\_JavaMiddle | 10745f2d440027312f7bc017a5f63010 | Да | - | RU-Moscow |  |  |
| sbc-k8s-worker-prod2 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-worker-0-stage1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-infra-prod-1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-worker-1-stage1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-worker-prod1 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-k8s-worker-prod0 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-nexus-01 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| sbc-jenkins-01 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |
| nexus | ru-moscow-1\_OpenShift | 1026bfce990026e02f64c0172ee8b343 | - | - | RU-Moscow |  |  |
| nexus | ru-moscow-1\_RHOS | 10196eb6b28026e02fddc017d18726ab | - | - | RU-Moscow |  |  |
| sbc-ipa-0 | ru-moscow-1 | 0bfa4ae35b8025a22fe4c017f4f35e1b | - | - | RU-Moscow |  |  |