ТБ Форум

АМИКОН

Делаем ядро безопасным: как не заблудиться в уязвимостях ядра Linux

Сергей Анненков

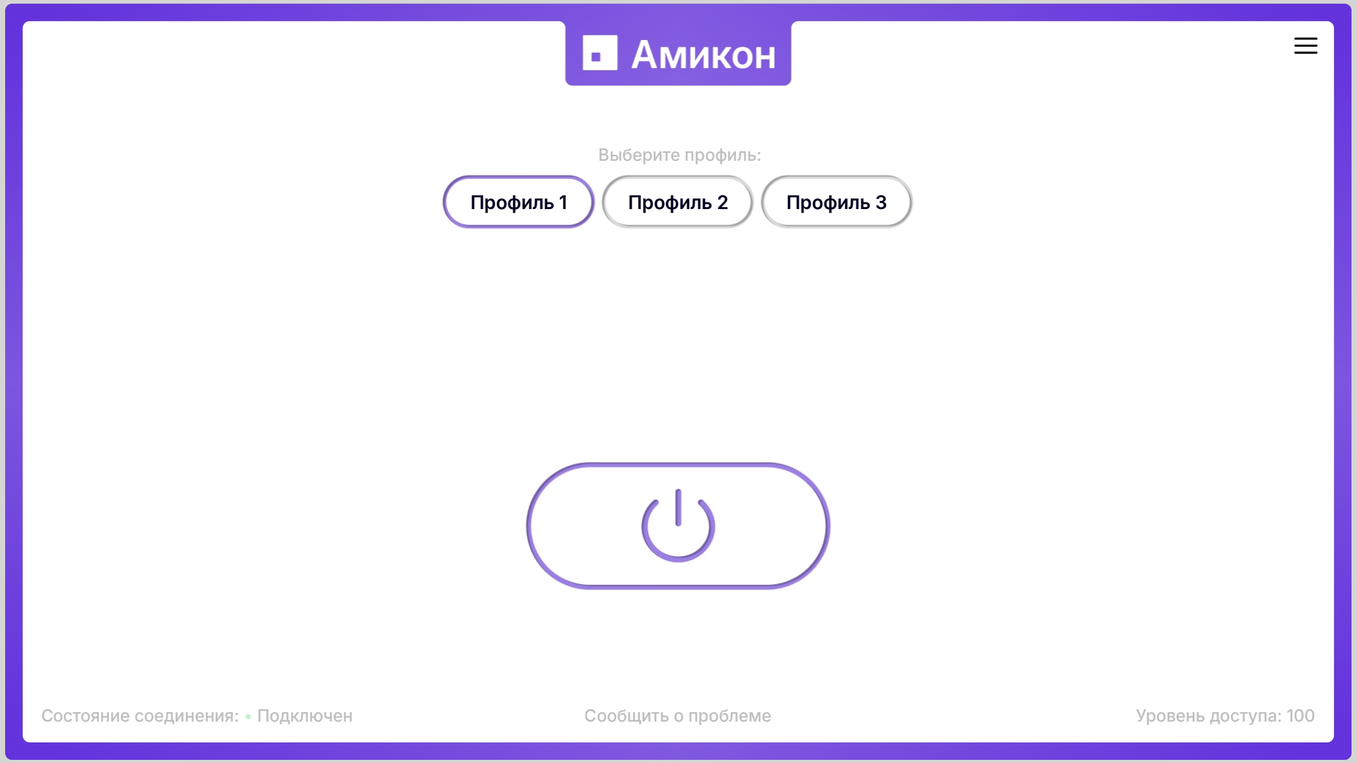
Руководитель Отдела Исследования Уязвимостей ПО.

amicon.ru

АМИКОН

Наши продукты

Амиконнект


Амикон
Выберите профиль:
Профиль 1
Профиль 2
Профиль 3
Состояние соединения: • Подключен
Сообщить о проблеме
Уровень доступа: 100

ФПСУ

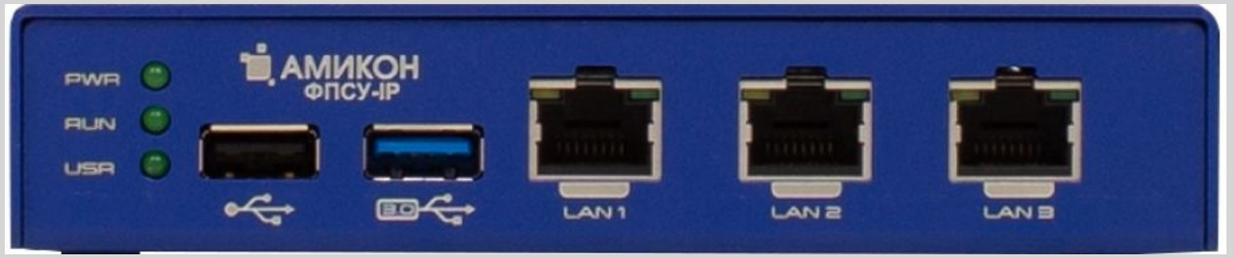
ULT6-10G

ФПСУ

STD3

ФПСУ

ORD4v2



АМИКОН

Экосистема

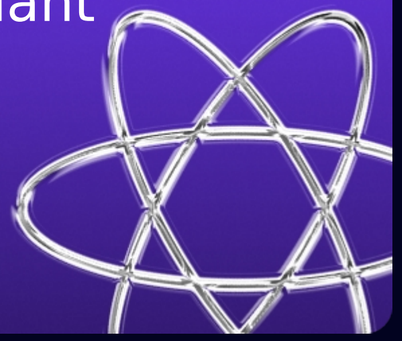
Экосистема

АМИКОН

NGFW

IDS/IPS

Quant



VPN Site to Site

VPN Клиент

SDK/API

Система управления

АМИКОН

Поддержание безопасности ядра

АМИКОН

Есть наша ветка ядра, задача:

1. Получить список CVE (DependencyTrack, cve-search, etc.)

- github.com/CVEProject/cvelistV5 – главный источник, машиночитаемый (.json)
- nvd.nist.gov – обеспечивает поиск по CPE, предоставляет API

2. Отфильтровать неактуальные уязвимости

- по версии ядра
- по описанию CVE и конфигурации сборки

3. Бекпортировать исправления уязвимостей

- вручную
- автоматически (tuxtape-cve-parser)

АМИКОН

Фильтрация по версии

Фильтрация по версии

АМИКОН

cvelistV5 / cves / 2024 / 25xxx / **CVE-2024-25744.json**

Code | Blame | 86 lines (86 loc) · 3.02 KB

```
20              "descriptions": [
21                  {
22                      "lang": "en",
23                      "value": "In the Linux kernel before 6.6.7, an untrusted VMM can trigger int80 syscall handlin
24                  }
25              ],
26              "affected": [
27                  {
28                      "vendor": "n/a",
29                      "product": "n/a",
30                      "versions": [
31                          {
32                              "version": "n/a",
33                              "status": "affected"
34                          }
35                      ]
36                  }
37              ],
38              "references": [
39                  {
40                      "url": "https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b82a8dbd
41                  },
```

Фильтрация по версии

АМИКОН

cvelistV5 / cves / 2024 / 26xxx / **CVE-2024-26581.json**

Code | Blame | 308 lines (308 loc) · 13.1 KB

```
19              "descriptions": [
20                  {
21                      "lang": "en",
22                      "value": "In the Linux kernel, the following vulnerability has been resolved:\n\nnetfilter: n
23                  }
24              ],
25              "affected": [
26                  {
27                      "product": "Linux",
28                      "vendor": "Linux",
29                      "defaultStatus": "unaffected",
30                      "repo": "https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git",
31                      "programFiles": [
32                          "net/netfilter/nft_set_rbtree.c"
33                      ],
34                      "versions": [
35                          {
36                              "version": "8284a79136c384059e85e278da2210b809730287",
37                              "lessThan": "c60d252949caf9aba537525195edae6bbabc35eb",
38                              "status": "affected",
39                              "versionType": "git"
40                          },
```

Фильтрация по версии

АМИКОН

```
85                    {
86                        "product": "Linux",
87                        "vendor": "Linux",
88                        "defaultStatus": "affected",
89                        "repo": "https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git",
90                        "programFiles": [
91                            "net/netfilter/nft_set_rbtree.c"
92                        ],
93                        "versions": [
94                            {
95                                "version": "6.5",
96                                "status": "affected"
97                            },
98                            {
99                                "version": "0",
100                               "lessThan": "6.5",
101                               "status": "unaffected",
102                               "versionType": "semver"
103                           },
104                           {
105                               "version": "5.4.269",
106                               "lessThanOrEqual": "5.4.*",
107                               "status": "unaffected",
108                               "versionType": "semver"
109                           },
110                           {
111                               "version": "5.10.210",
112                               "lessThanOrEqual": "5.10.*",
113                               "status": "unaffected",
114                               "versionType": "semver"
115                           },
```

Фильтрация по версии

АМИКОН

kernel.org Added as CVE Numbering Authority (CNA)

Links that redirect to external websites will open a new window or tab depending on the web browser used.

News February 13, 2024

kernel.org is now a **CVE Numbering Authority (CNA)** for any vulnerabilities in the Linux kernel as listed on kernel.org, excluding end-of-life (EOL) versions.

To date, **361 CNAs** (359 CNAs and 2 CNA-LRs) from **40 countries** and 1 no country affiliation have partnered with the CVE Program. CNAs are organizations from around the world that are authorized to assign **CVE Identifiers (CVE IDs)** and publish **CVE Records** for vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. kernel.org is the 193rd CNA from USA.

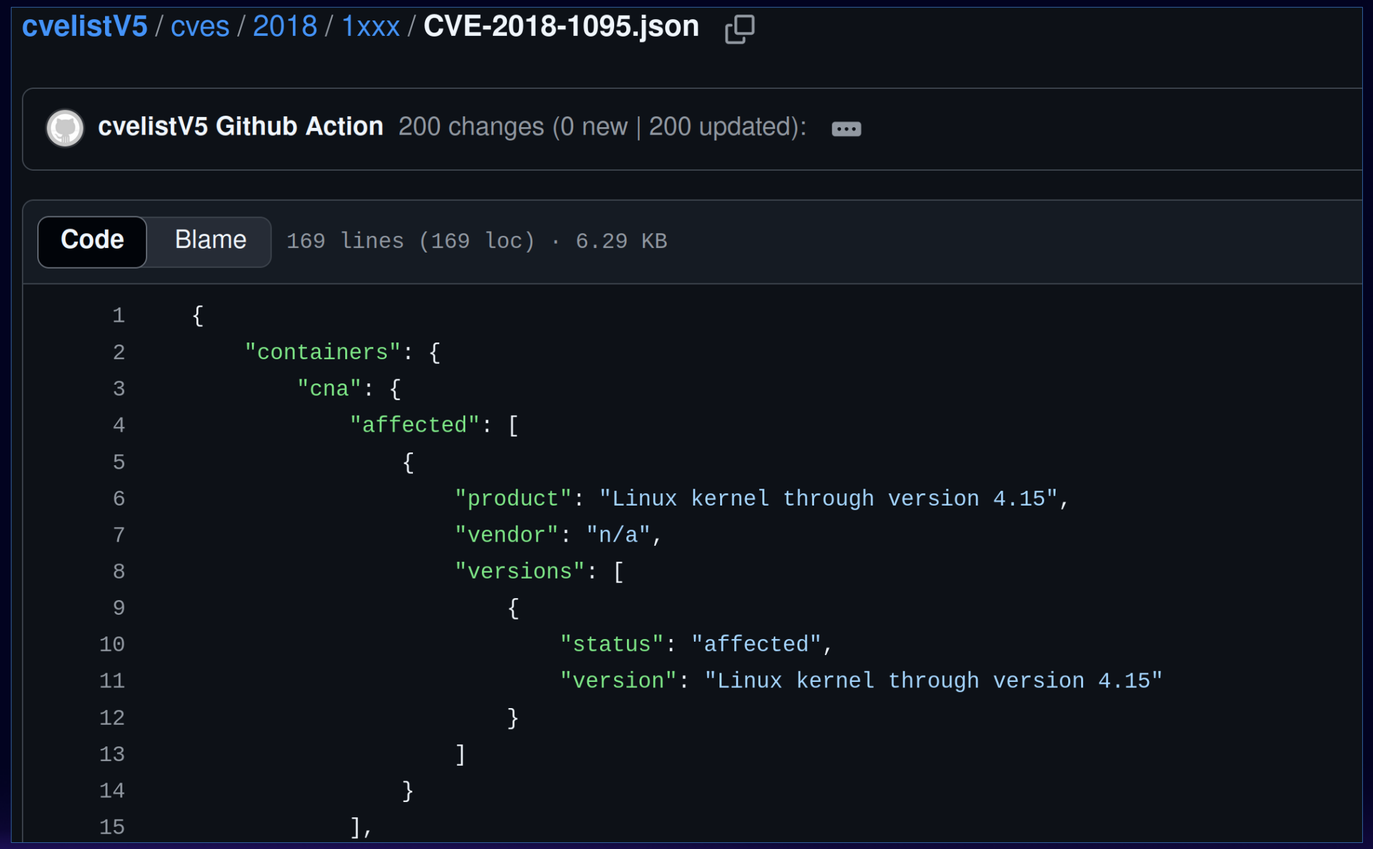
kernel.org’s Root is the **MITRE Top-Level Root**.

АМИКОН

Начиная с 13 февраля 2024 г. затронутые CVE версии ядра указываются через коммиты и точные версии, источник:

- git.kernel.org/pub/scm/linux/security/vulns.git

До этого у многих CVE указан только исправляющий релиз.



АМИКОН

Сторонние трекеры CVE

Сторонние трекеры CVE

АМИКОН

В сторонних трекерах можно найти коммиты, внесшие/исправляющие уязвимость, более точные версии, комментарии.

Некоторые из них:

- bdu.fstec.ru/ - Банк данных угроз безопасности информации - ФСТЭК
- github.com/nluedtke/linux_kernel_cves - используется в Yocto, заморожен
- gitlab.com/cip-project/cip-kernel/cip-kernel-sec – включает в себя в том числе данные из
  - salsa.debian.org/kernel-team/kernel-sec (проект Debian)
  - git.launchpad.net/ubuntu-cve-tracker (проект Ubuntu)

CIP-kernel-sec позволяет добавлять другие ветки для автоматического поиска исправляющих коммитов / регрессий.

Сторонние трекеры CVE - CIP-kernel-sec

АМИКОН

CVE-2018-1095.yml

```yaml
description: |-
  The ext4_xattr_check_entries function in fs/ext4/xattr.c in the Linux
  kernel through 4.15.15 does not properly validate xattr sizes, which causes
  misinterpretation of a size as an error code, and consequently allows
  attackers to cause a denial of service (get_acl NULL pointer dereference
  and system crash) via a crafted ext4 image.
references:
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1095
- https://bugzilla.kernel.org/show_bug.cgi?id=199185
- https://usn.ubuntu.com/usn/usn-3695-1
- https://usn.ubuntu.com/usn/usn-3695-2
- https://ubuntu.com/security/notices/USN-3695-1
- https://ubuntu.com/security/notices/USN-3695-2
- https://www.cve.org/CVERecord?id=CVE-2018-1095
comments:
  debian/carnil: Introduced with e50e5129f384ae282adebfb561189cdb19b81cee (4.13-rc1)
reporters:
- Wen Xu
introduced-by:
  mainline: [e50e5129f384ae282adebfb561189cdb19b81cee]
fixed-by:
  debian/buster-security: ['version:debian/4.16.5-1']
  mainline: [ce3fd194fcc6fbdc00ce095a852f22df97baa401]
  stable/4.14: [a57eb14b740e6175aff8b8941bec628403992dfa]
  stable/4.16: [d97c42e8f9bc9054101d04d715ff322379bfa1c9]
  ubuntu/bionic: [96f89abf766d063c18fc9572ebb8afb938c17856]
```

Сторонние трекеры CVE – БДУ ФСТЭК

АМИКОН

Извлечение версий ядра для заданных CVE из данных формата XML.

```
vul_matches = root.findall(f"./vul/identifiers/identifier[@type='CVE'][.='{cve_value}']/../..")

if not vul_matches:
    print(f"{cve_value}\tBDU value not found")
    continue

for vul in vul_matches:
    # bdu = vul['identifier']
    bdu = vul[0]

    ver_strings = set()
    for v in vul.iterfind("./vulnerable_software/soft/name[.='Linux']/../version"):
        ver_strings.add(v.text)

    # (text, version_1, version_2, closed)
    ver_list = [(v,) + parse_version(v) for v in ver_strings]
    # сортируем кортежи по длине, чтобы версии вида X.Y оказались в конце списка
    ver_list.sort(key=lambda ver: len(ver[2]), reverse=True)

    ver_text = check_version(version, ver_list)

    output = f"{cve_value}\t{bdu.text}"
    if ver_text:
        output += f"\tVersion: {ver_text}"
    print(output)
```

АМИКОН

Фильтрация по конфигурации

Фильтрация по конфигурации

АМИКОН

- автоматическая - анализ сборки ядра на участие в компиляции коммита, вносящего уязвимость (интересная идея, трудоёмко)

- полуавтоматическая - простой анализ конфигурации - предлагаем человеку вариант выключенной опции по совпадению токенов с описанием уязвимости

```
    "CVE-2018-19854": {
      "name": "CVE-2018-19854",
      "description": "An issue was discovered in the Linux kernel before 4.19.3. crypto_report_one() and
related functions in crypto/crypto_user.c (the crypto user configuration API) do not fully initialize
structures that are copied to userspace, potentially leaking sensitive memory to user programs. NOTE: this is
a CVE-2013-2547 regression but with easier exploitability because the attacker does not need a capability
(however, the system must have the CONFIG_CRYPTO_USER kconfig option).",
      "applicable": false,
      "comment": "Данный CVE не актуален: не задействован параметр конфигурации CONFIG_CRYPTO_USER_API"
    },
```

- ручная - поиск по ключевым словам в описаниях - bluetooth, wifi, etc.

АМИКОН

Результаты

Результаты

АМИКОН

- фильтрация по версиям из CIP-kernel-sec – 42% списка CVE
- фильтрация по версиям из БДУ – 60% списка CVE
- фильтрация по конфигурации – 25% списка CVE
- актуальных CVE – 2.5%

АМИКОН

Спасибо за внимание!