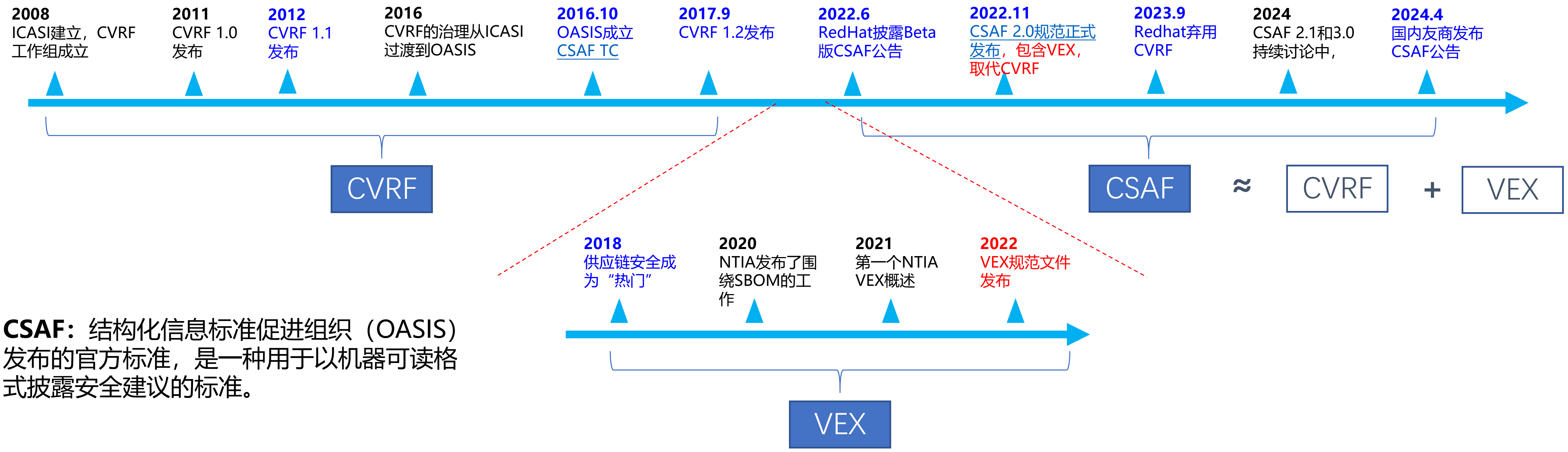
openEuler支持CSAF格式漏洞公告

openEuler安全委员会

开放原子开源基金会
OPENATOM FOUNDATION | openEuler

CSAF标准是CVRF标准的继任者，同时也是VEX标准的具体实现形式之一



2008
ICASI建立，CVRF工作组成立

2011
CVRF 1.0发布

2012
CVRF 1.1发布

2016
CVRF的治理从ICASI过渡到OASIS

2016.10
OASIS成立CSAF TC

2017.9
CVRF 1.2发布

2022.6
RedHat披露Beta版CSAF公告

2022.11
CSAF 2.0规范正式发布，包含VEX，取代CVRF

2023.9
Redhat弃用CVRF

2024
CSAF 2.1和3.0持续讨论中，

2024.4
国内友商发布CSAF公告

CVRF

CSAF ≈ CVRF + VEX

2018
供应链安全成为“热门”

2020
NTIA发布了围绕SBOM的工作

2021
第一个NTIA VEX概述

2022
VEX规范文件发布

VEX

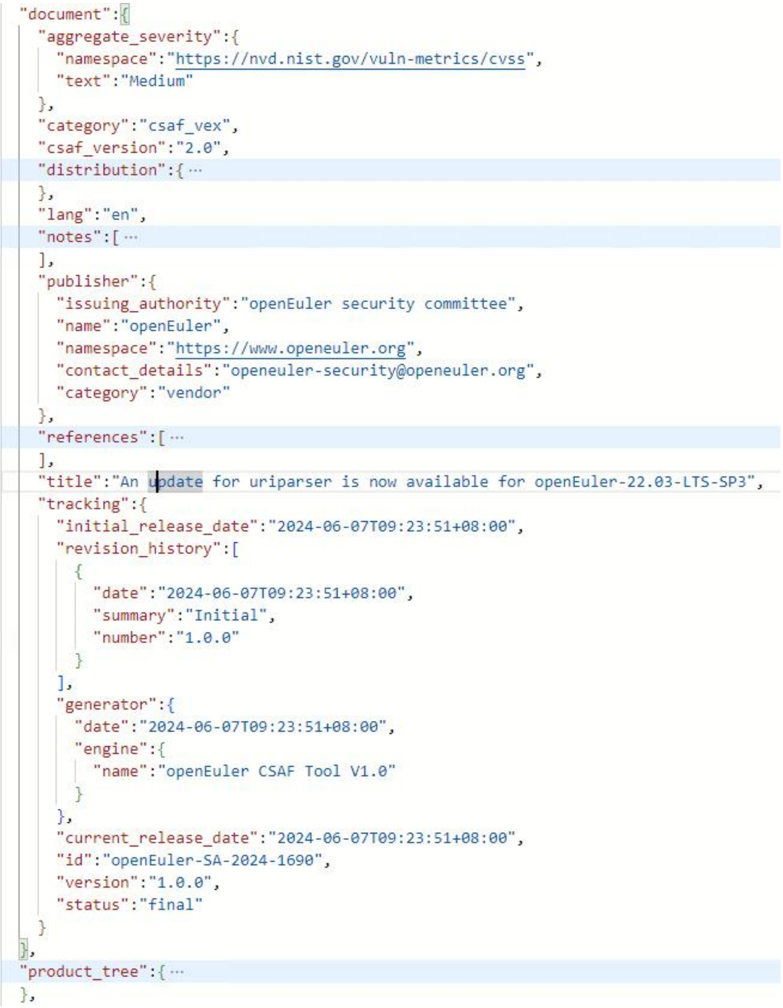
CSAF：结构化信息标准促进组织（OASIS）发布的官方标准，是一种用于以机器可读格式披露安全建议的标准。

CSAF发展历程：

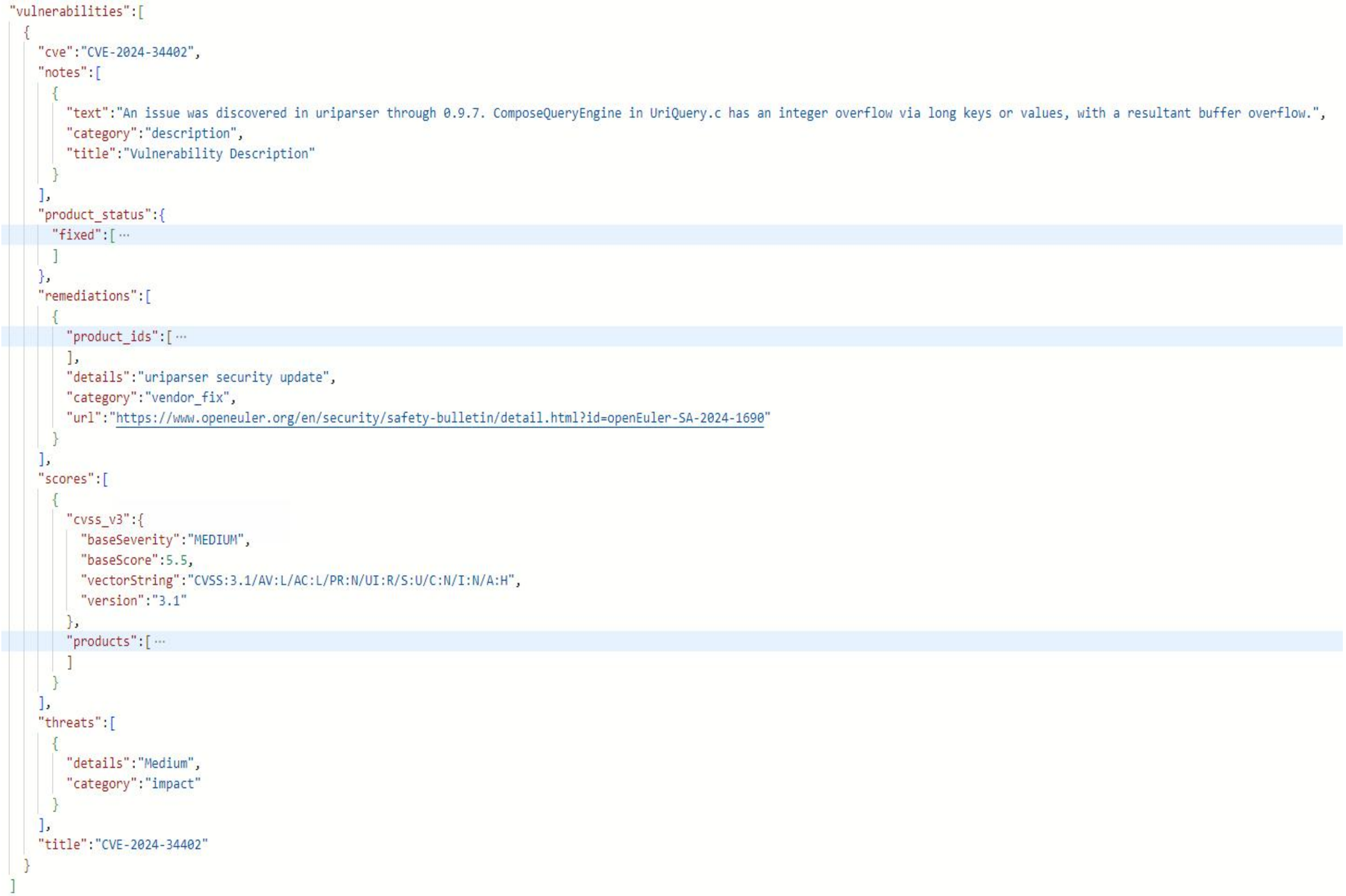
- ➢ CVRF 是发布安全公告SA的行业标准格式，最早由ICASI 发布，2011年和2012年分别发布1.0和1.1版本；
- ➢ 2016年，CVRF的治理工作由OASIS接管，在2017年发布1.2版本；
- ➢ 2018~2022年，供应链安全成为“热门”，NTIA主导发布了VEX标准，作为SBOM的“伴侣制品”；
- ➢ 2022年，OASIS正式发布CSAF 2.0规范，包含VEX的实现，取代CVRF；
- ➢ 2023年9月，Redhat停止发布CVRF格式的安全公告，用CSAF替代；
- ➢ 2024年4月，国内友商发布CSAF格式安全公告；

CVRF：通用漏洞报告框架
CSAF：通用安全通告框架
ICASI：互联网安全促进行业联盟
OASIS：结构化信息标准推动组织
VEX：漏洞利用交换
NTIA：美国国家通信和信息管理局

安全公告维度的CSAF



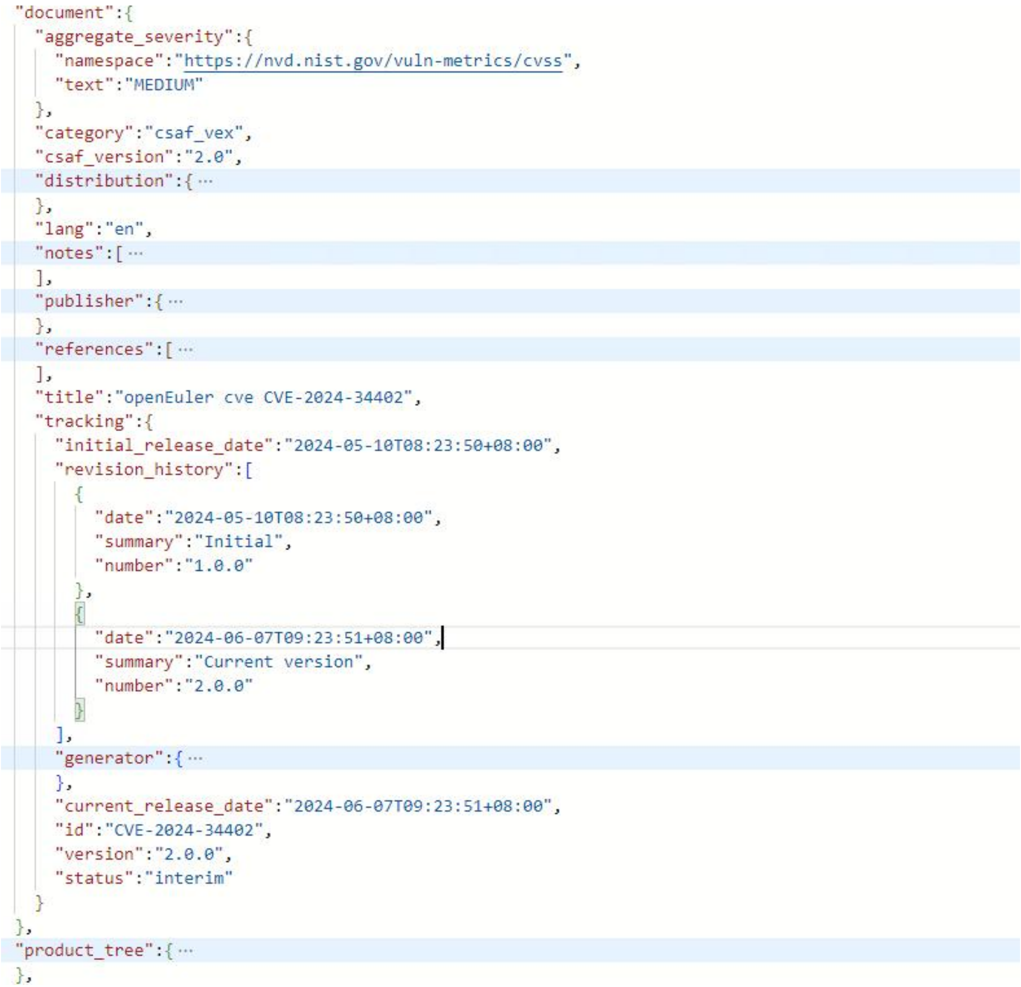
```
"document":{
  "aggregate_severity":{
    "namespace":"https://nvd.nist.gov/vuln-metrics/cvss",
    "text":"Medium"
  },
  "category":"csaf_vex",
  "csaf_version":"2.0",
  "distribution":{ ···
  },
  "lang":"en",
  "notes":[ ···
  ],
  "publisher":{
    "issuing_authority":"openEuler security committee",
    "name":"openEuler",
    "namespace":"https://www.openeuler.org",
    "contact_details":"openeuler-security@openeuler.org",
    "category":"vendor"
  },
  "references":[ ···
  ],
  "title":"An update for uriparser is now available for openEuler-22.03-LTS-SP3",
  "tracking":{
    "initial_release_date":"2024-06-07T09:23:51+08:00",
    "revision_history":[
      {
        "date":"2024-06-07T09:23:51+08:00",
        "summary":"Initial",
        "number":"1.0.0"
      }
    ],
    "generator":{
      "date":"2024-06-07T09:23:51+08:00",
      "engine":{
        "name":"openEuler CSAF Tool V1.0"
      }
    },
    "current_release_date":"2024-06-07T09:23:51+08:00",
    "id":"openEuler-SA-2024-1690",
    "version":"1.0.0",
    "status":"final"
  }
},
"product_tree":{ ···
},
```



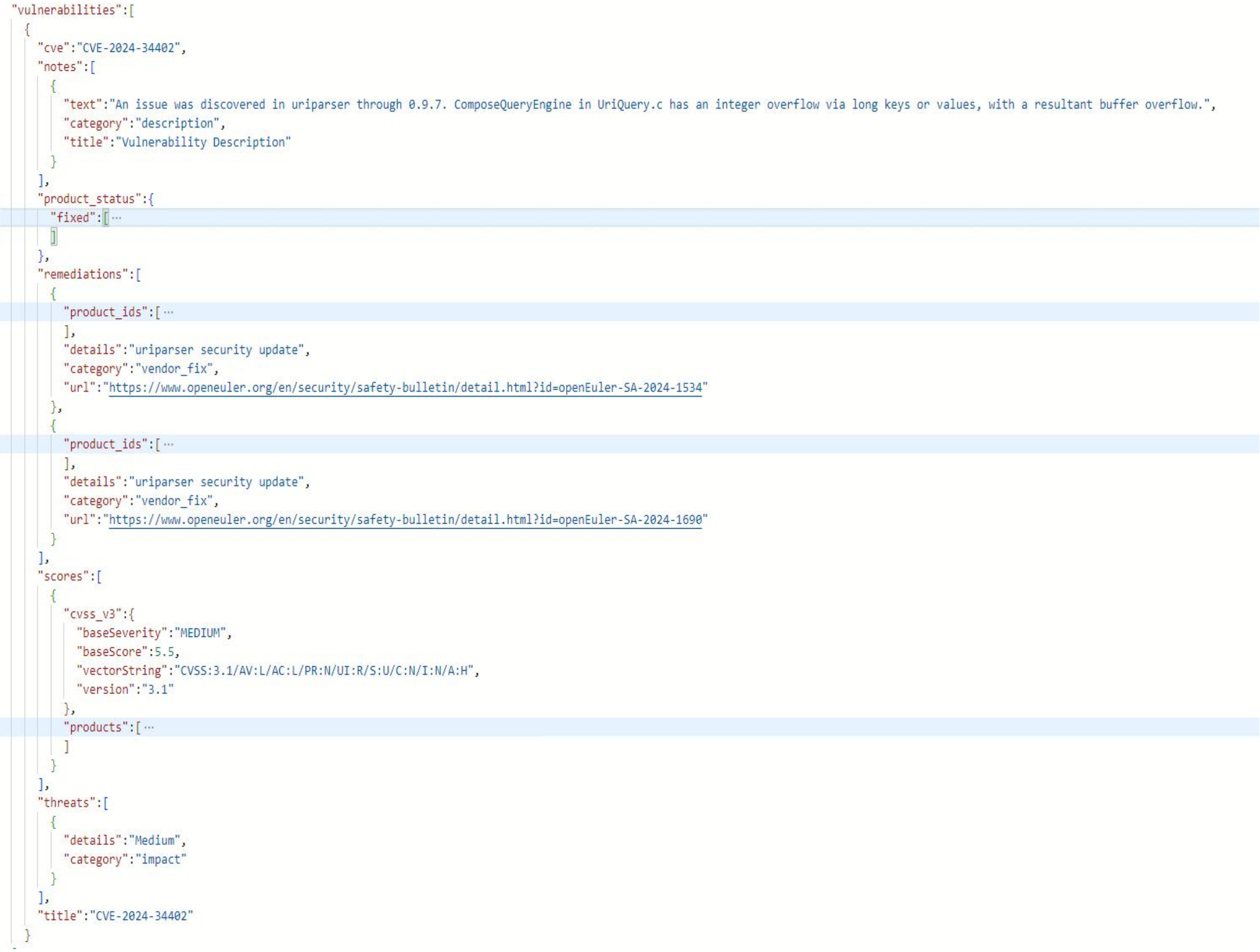
```
"vulnerabilities":[
  {
    "cve":"CVE-2024-34402",
    "notes":[
      {
        "text":"An issue was discovered in uriparser through 0.9.7. ComposeQueryEngine in UriQuery.c has an integer overflow via long keys or values, with a resultant buffer overflow.",
        "category":"description",
        "title":"Vulnerability Description"
      }
    ],
    "product_status":{
      "fixed":[ ···
      ]
    },
    "remediations":[
      {
        "product_ids":[ ···
        ],
        "details":"uriparser security update",
        "category":"vendor_fix",
        "url":"https://www.openeuler.org/en/security/safety-bulletin/detail.html?id=openEuler-SA-2024-1690"
      }
    ],
    "scores":[
      {
        "cvss_v3":{
          "baseSeverity":"MEDIUM",
          "baseScore":5.5,
          "vectorString":"CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H",
          "version":"3.1"
        },
        "products":[ ···
        ]
      }
    ],
    "threats":[
      {
        "details":"Medium",
        "category":"impact"
      }
    ],
    "title":"CVE-2024-34402"
  }
]
```

安全公告维度的CSAF文件是从安全公告维度，对给定的产品构建已修复的漏洞映射。
主要分为三部分：
1）document：对整个csaf文档的类型、语言、涉及链接、发布历史等概述
2）product_tree:构建本次安全公告中涉及到的产品信息
3）vulnerabilities：披露本次安全公告中涉及的各个cve的详情、评分、产品状态、修复说明等

CVE维度的CSAF



```
"document":{
  "aggregate_severity":{
    "namespace":"https://nvd.nist.gov/vuln-metrics/cvss",
    "text":"MEDIUM"
  },
  "category":"csaf_vex",
  "csaf_version":"2.0",
  "distribution":{ ···
  },
  "lang":"en",
  "notes":[ ···
  ],
  "publisher":{ ···
  },
  "references":[ ···
  ],
  "title":"openEuler cve CVE-2024-34402",
  "tracking":{
    "initial_release_date":"2024-05-10T08:23:50+08:00",
    "revision_history":[
      {
        "date":"2024-05-10T08:23:50+08:00",
        "summary":"Initial",
        "number":"1.0.0"
      },
      {
        "date":"2024-06-07T09:23:51+08:00",
        "summary":"Current version",
        "number":"2.0.0"
      }
    ],
    "generator":{ ···
    },
    "current_release_date":"2024-06-07T09:23:51+08:00",
    "id":"CVE-2024-34402",
    "version":"2.0.0",
    "status":"interim"
  }
},
"product_tree":{ ···
},
```



```
"vulnerabilities":[
  {
    "cve":"CVE-2024-34402",
    "notes":[
      {
        "text":"An issue was discovered in uriparser through 0.9.7. ComposeQueryEngine in UriQuery.c has an integer overflow via long keys or values, with a resultant buffer overflow.",
        "category":"description",
        "title":"Vulnerability Description"
      }
    ],
    "product_status":{
      "fixed":[ ···
      ]
    },
    "remediations":[
      {
        "product_ids":[ ···
        ],
        "details":"uriparser security update",
        "category":"vendor_fix",
        "url":"https://www.openeuler.org/en/security/safety-bulletin/detail.html?id=openEuler-SA-2024-1534"
      },
      {
        "product_ids":[ ···
        ],
        "details":"uriparser security update",
        "category":"vendor_fix",
        "url":"https://www.openeuler.org/en/security/safety-bulletin/detail.html?id=openEuler-SA-2024-1690"
      }
    ],
    "scores":[
      {
        "cvss_v3":{
          "baseSeverity":"MEDIUM",
          "baseScore":5.5,
          "vectorString":"CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H",
          "version":"3.1"
        },
        "products":[ ···
        ]
      }
    ],
    "threats":[
      {
        "details":"Medium",
        "category":"impact"
      }
    ],
    "title":"CVE-2024-34402"
  }
```

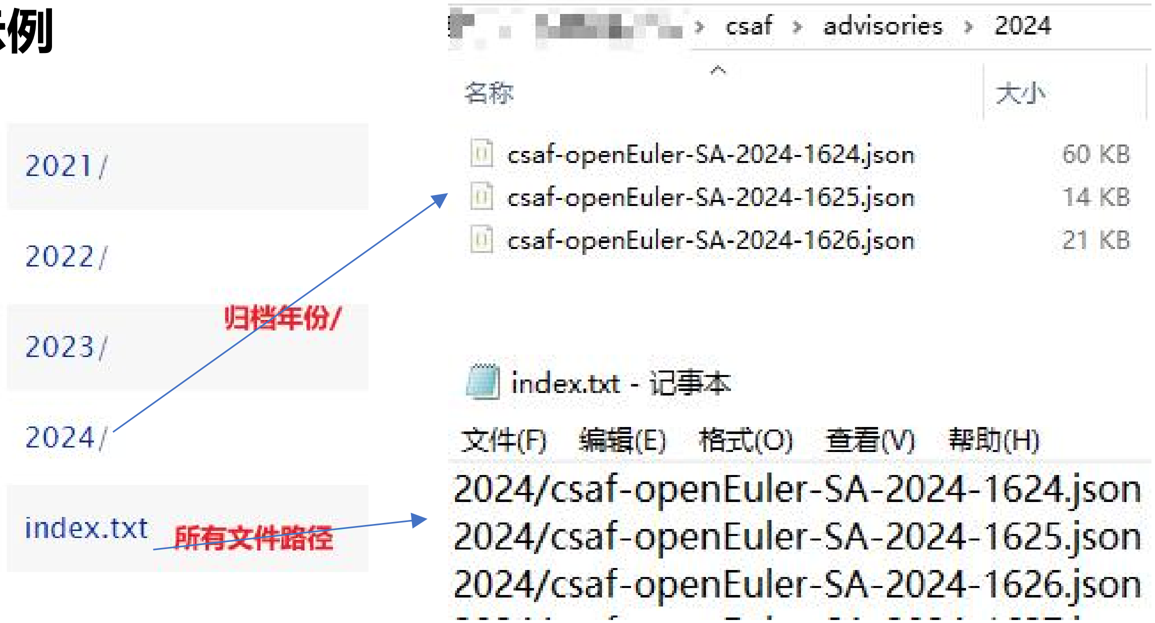
CVE维度的CSAF文件是从漏洞维度，披露产品影响程度信息和修补信息
主要分为三部分：
1）document：对整个csaf文档的类型、语言、涉及链接、发布历史等概述
2）product_tree:构建该cve涉及到的产品信息
3）vulnerabilities：披露该cve详情、评分、产品状态、修复说明等。

openEuler社区支持CSAF漏洞披露格式

①安全公告维度CSAF

针对给定产品构建已修复漏洞的映射归档路径：
https://repo.openeuler.org/security/data/csaf/advisories/

示例



2021/
2022/
2023/
2024/
index.txt
归档年份/
所有文件路径
[redacted] › csaf › advisories › 2024
名称
大小
index.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

名称	大小
csaf-openEuler-SA-2024-1624.json	60 KB
csaf-openEuler-SA-2024-1625.json	14 KB
csaf-openEuler-SA-2024-1626.json	21 KB

```
2024/csaf-openEuler-SA-2024-1624.json
2024/csaf-openEuler-SA-2024-1625.json
2024/csaf-openEuler-SA-2024-1626.json
```

计划：

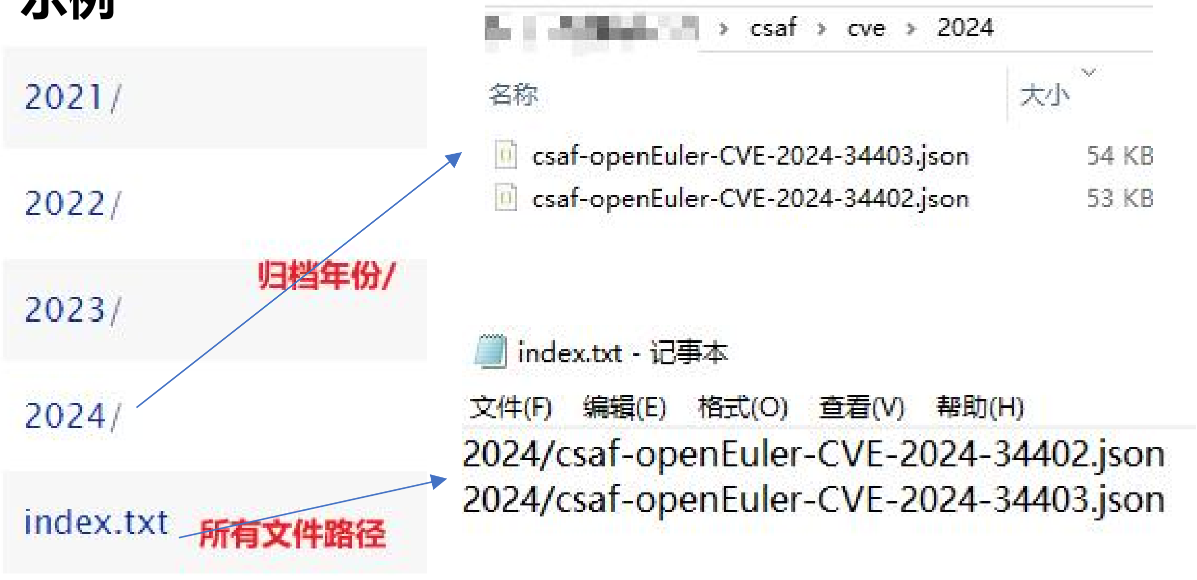
1、从7.5号开始，社区对新增漏洞支持CSAF格式的安全公告；

2、在9.30号前补齐历史漏洞的CSAF格式的安全公告；

②CVE维度CSAF

包含每个漏洞的产品影响程度信息，可以补充构建给定产品中未修复漏洞的映射归档路径：
https://repo.openeuler.org/security/data/csaf/cve/

示例



名称	大小
csaf-openEuler-CVE-2024-34403.json	54 KB
csaf-openEuler-CVE-2024-34402.json	53 KB

```
2024/csaf-openEuler-CVE-2024-34402.json
2024/csaf-openEuler-CVE-2024-34403.json
```

计划：

1、在11.1号前完成不受影响漏洞及其原因的支持和披露，发布CVE维度的CSAF；

决策和建议

- 同意openEuler社区支持CSAF格式的漏洞公告；

THANKS

开放原子开源基金会
OPENATOM FOUNDATION | openEuler