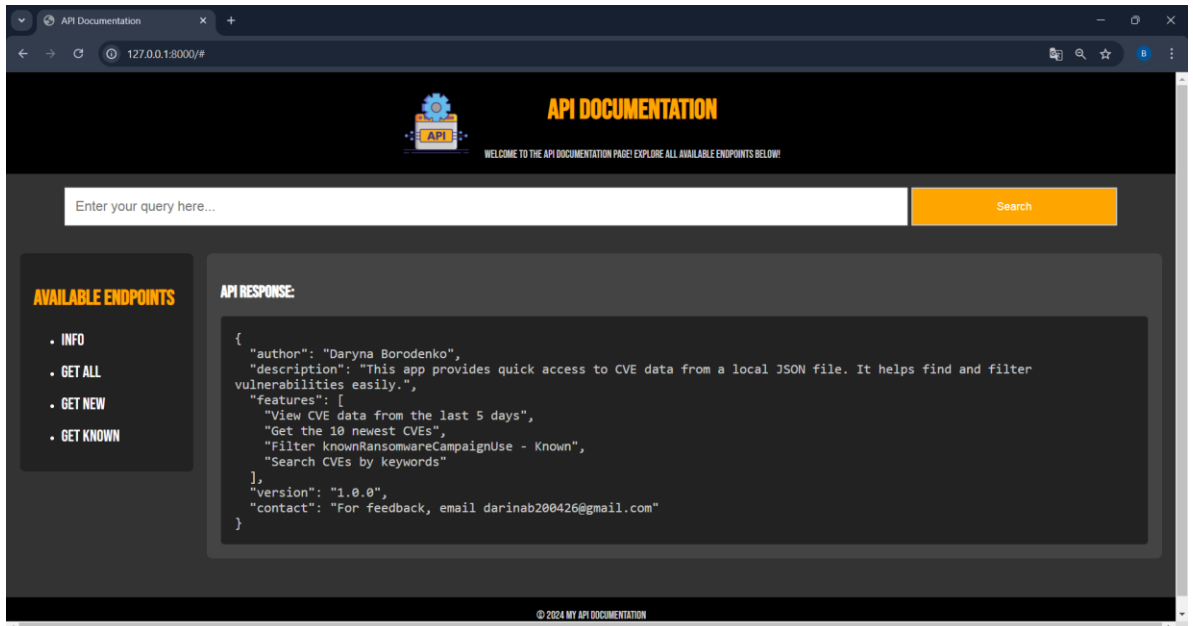


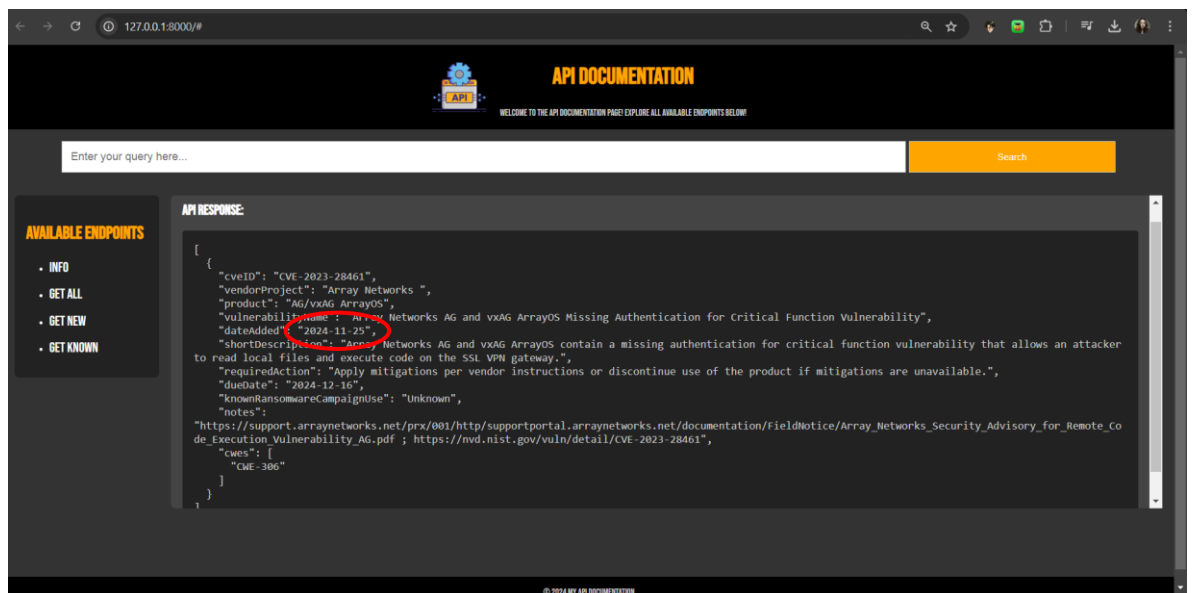
РЕЗУЛЬТАТ

uvicorn main:app --reload

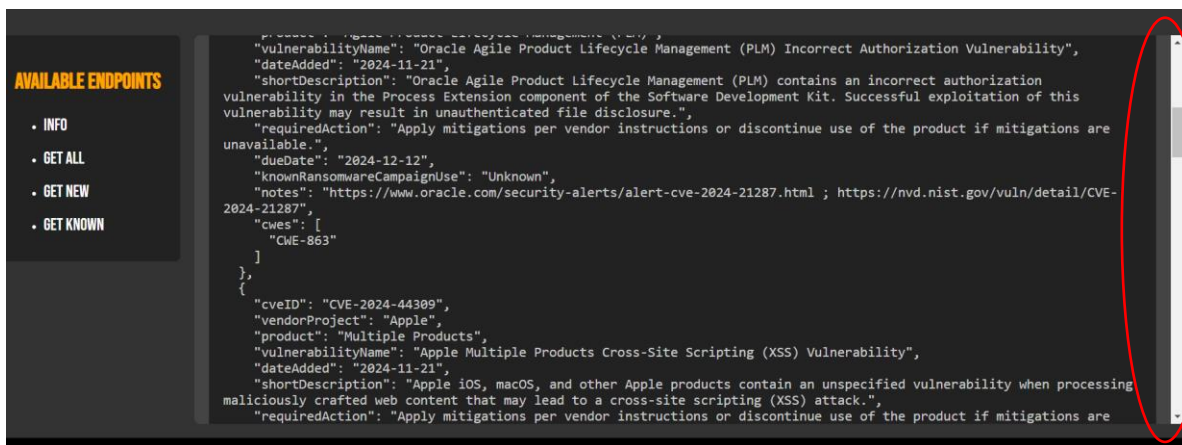
INFO



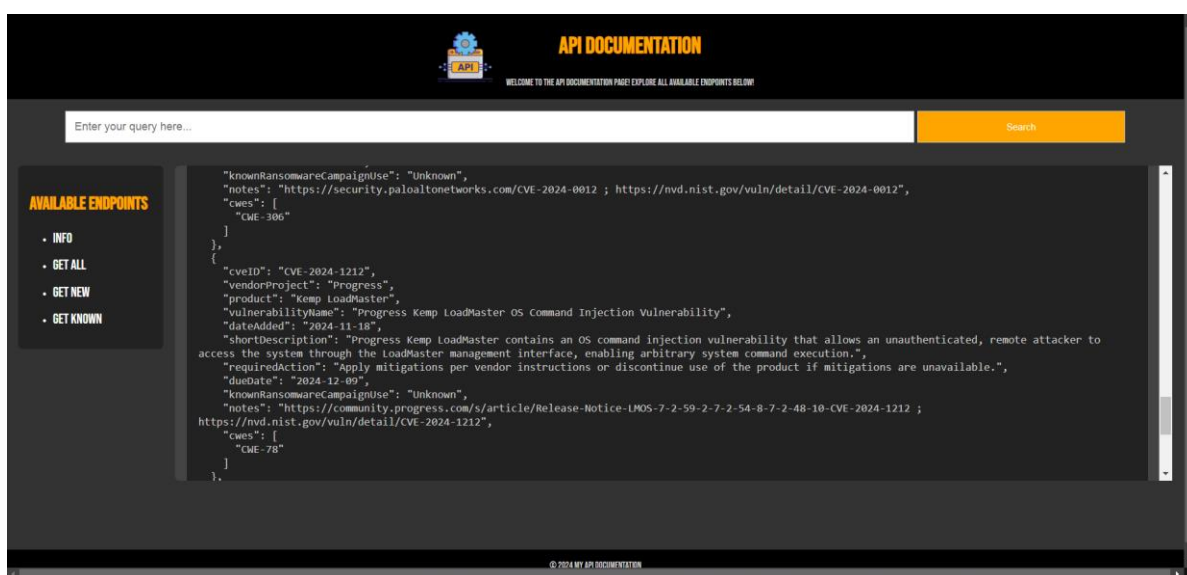
GET ALL (оскільки в нас файл і інформація не оновлюється, то я взяла за останні 10 днів по дефолту)



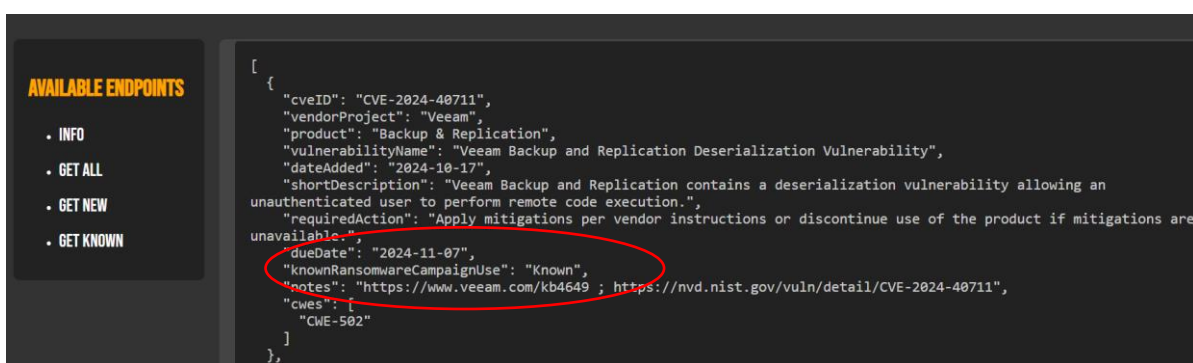
Наприклад, якщо я виставляю 15 днів, то вже більше виводить інформації



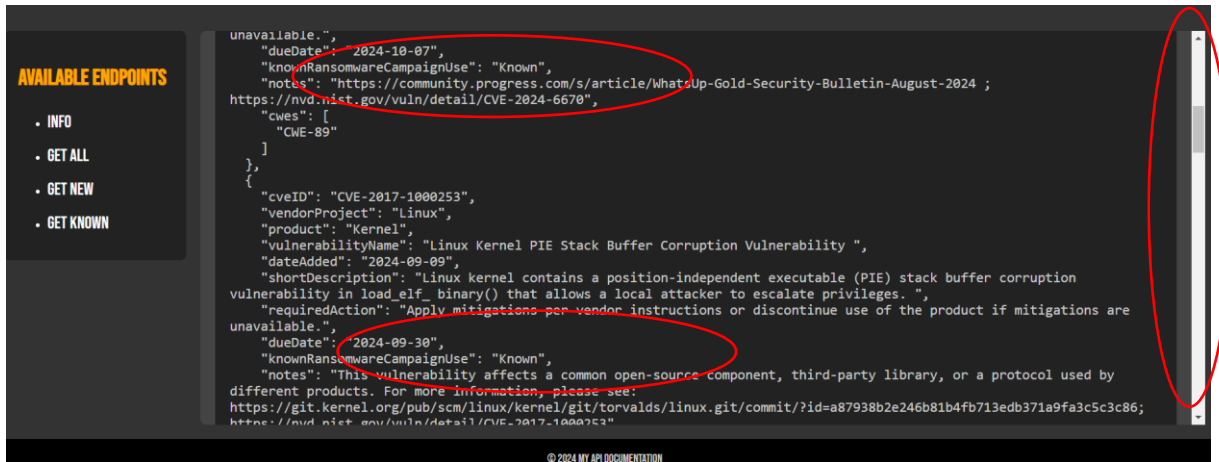
GET NEW Виводить чітко 10 найновіших CVE



GET KNOWN Виводить CVE в яких knownRansomwareCampaignUse – **Known**

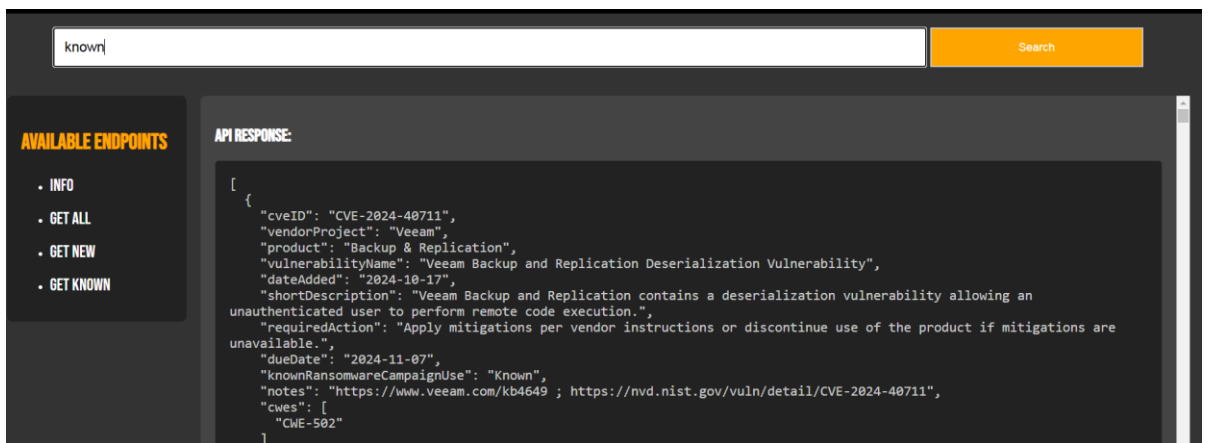


І так далі....



```
unavailable.",
  "dueDate": "2024-10-07",
  "knownRansomwareCampaignUse": "Known",
  "notes": "https://community.progress.com/s/article/WhatUp-Gold-Security-Bulletin-August-2024 ;
https://nvd.nist.gov/vuln/detail/CVE-2024-6670",
  "cves": [
    "CVE-89"
  ]
},
{
  "cveID": "CVE-2017-1000253",
  "vendorProject": "Linux",
  "product": "Kernel",
  "vulnerabilityName": "Linux Kernel PIE Stack Buffer Corruption Vulnerability ",
  "dateAdded": "2024-09-09",
  "shortDescription": "Linux kernel contains a position-independent executable (PIE) stack buffer corruption
vulnerability in load_elf_binary() that allows a local attacker to escalate privileges. ",
  "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are
unavailable.",
  "dueDate": "2024-09-30",
  "knownRansomwareCampaignUse": "Known",
  "notes": "This vulnerability affects a common open-source component, third-party library, or a protocol used by
different products. For more information, please see:
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=a87938b2e246b81b4fb713edb371a9fa3c5c3c86;
https://nvd.nist.gov/vuln/detail/CVE-2017-1000253"
}
```

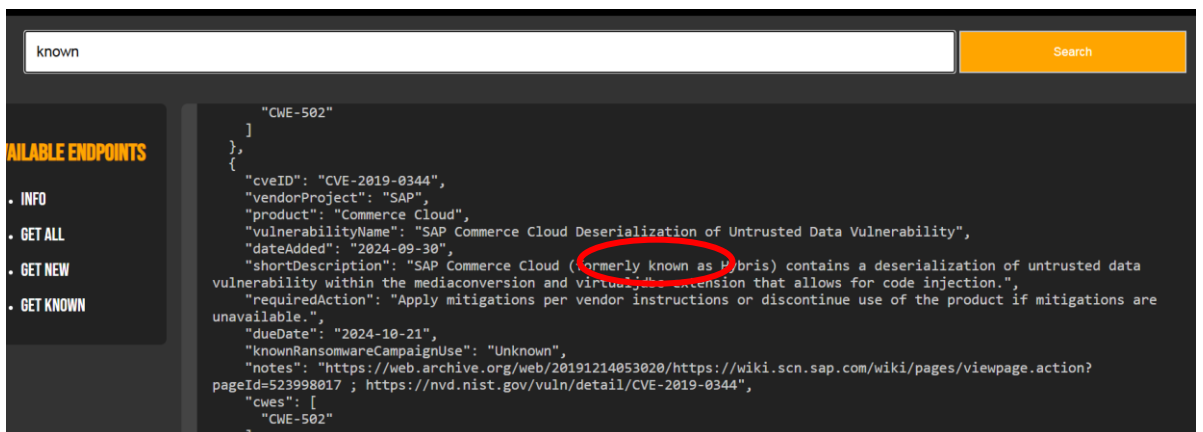
SEARCH – за певним ключовим словом шукає.



```
[
{
  "cveID": "CVE-2024-40711",
  "vendorProject": "Veeam",
  "product": "Backup & Replication",
  "vulnerabilityName": "Veeam Backup and Replication Deserialization Vulnerability",
  "dateAdded": "2024-10-17",
  "shortDescription": "Veeam Backup and Replication contains a deserialization vulnerability allowing an
unauthenticated user to perform remote code execution.",
  "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are
unavailable.",
  "dueDate": "2024-11-07",
  "knownRansomwareCampaignUse": "Known",
  "notes": "https://www.veeam.com/kb4649 ; https://nvd.nist.gov/vuln/detail/CVE-2024-40711",
  "cves": [
    "CVE-502"
  ]
}
```

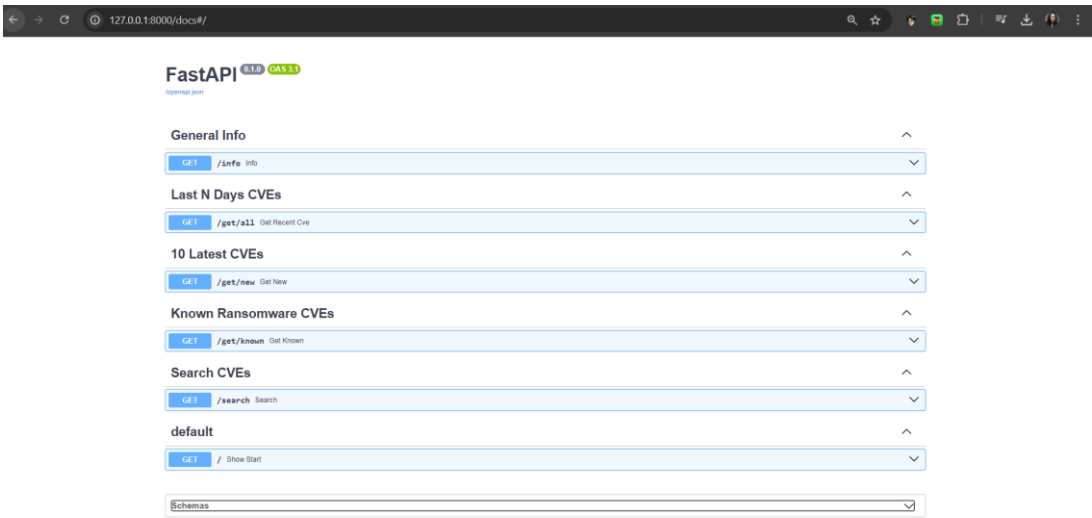
if **re.search(rf'\b{re.escape(query)}\b', json.dumps(cve), re.IGNORECASE)**

Перевіряє, чи існує певний **query** як окреме слово (а не як частина іншого слова, як known unknown, наприклад). Забезпечує нечутливість до регістру.

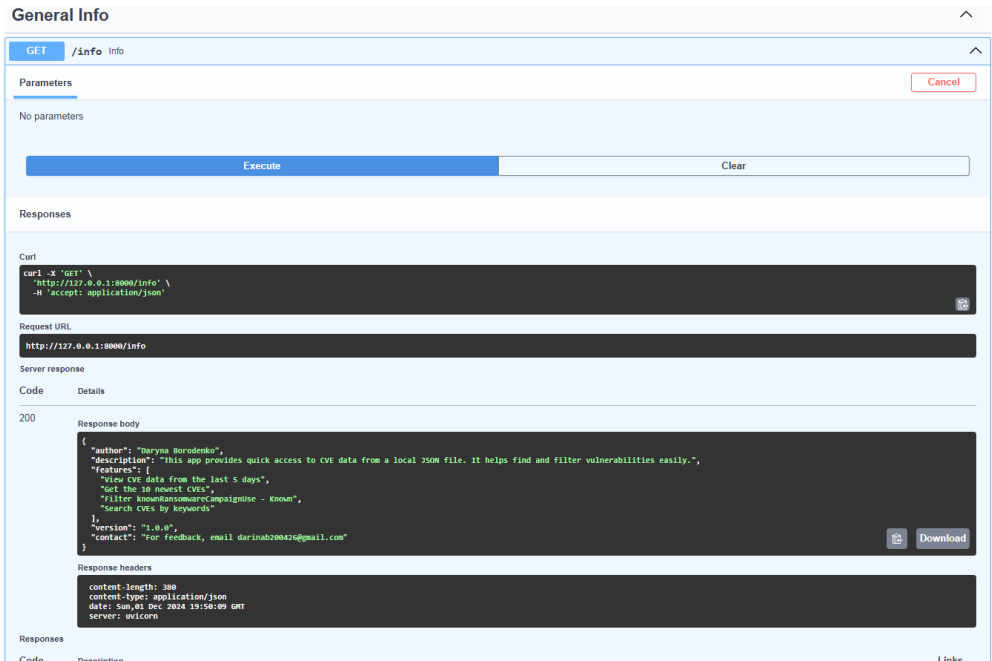


```
"CVE-502"
},
{
  "cveID": "CVE-2019-0344",
  "vendorProject": "SAP",
  "product": "Commerce Cloud",
  "vulnerabilityName": "SAP Commerce Cloud Deserialization of Untrusted Data Vulnerability",
  "dateAdded": "2024-09-30",
  "shortDescription": "SAP Commerce Cloud (formerly known as Hybris) contains a deserialization of untrusted data
vulnerability within the mediaconversion and virtuajob extension that allows for code injection.",
  "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are
unavailable.",
  "dueDate": "2024-10-21",
  "knownRansomwareCampaignUse": "Unknown",
  "notes": "https://web.archive.org/web/20191214053020/https://wiki.scn.sap.com/wiki/pages/viewpage.action?
pageId=523998017 ; https://nvd.nist.gov/vuln/detail/CVE-2019-0344",
  "cves": [
    "CVE-502"
  ]
}
```

fastapi dev main.py

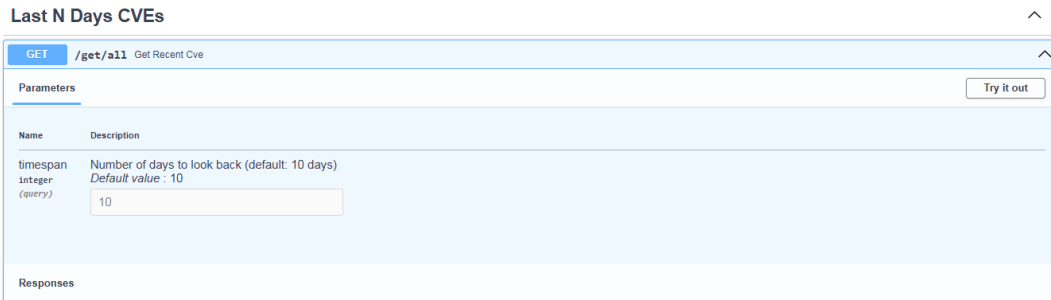


INFO



GET ALL

По дефолту 10, бо з 5 буде 0.



Ставлю 15 для прикладу

Last N Days CVEs

GET

/get/all

Get Recent Cve

Parameters

Cancel

Name	Description
timespan integer (query)	Number of days to look back (default: 15 days)

15

Execute

Parameters

Clear

Name	Description
timespan integer (query)	Number of days to look back (default: 10 days)

15

Execute

Responses

Curl

curl -X 'GET' \

Request URL

http://127.0.0.1:8000/get/all?timespan=15

Server response

Code

Details

200

Response body

[{"cveID": "CVE-2023-28461", "vendorProject": "Array Networks ", "product": "Array Networks AG and vxAG ArrayOS Missing Authentication for Critical Function Vulnerability", "vulnerabilityName": "Array Networks AG and vxAG ArrayOS Missing Authentication for Critical Function Vulnerability", "dateAdded": "2024-11-25", "shortDescription": "Array Networks AG and vxAG ArrayOS contain a missing authentication for critical function vulnerability that allows an attacker to read local files and execute code on the SSL VPN gateway.", "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.", "date": "2024-12-16", "knownHansomwareCampaignUse": "Unknown", "notes": "https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_Remote_Code_Execution_Vulnerability_Ag.pdf ; https://nvd.nist.gov/vuln/detail/CVE-2023-28461", "cves": [{"cve": "CVE-306"}]}, {"cveID": "CVE-2024-21287", "vendorProject": "Oracle", "product": "Agile Product Lifecycle Management (PLM)", "vulnerabilityName": "Oracle Agile Product Lifecycle Management (PLM) Incorrect Authorization Vulnerability", "dateAdded": "2024-11-21", "shortDescription": "Oracle Agile Product Lifecycle Management (PLM) contains an incorrect authorization vulnerability in the Process Extension component of the Software Development Kit."}]

GET NEW

10 Latest CVEs

GET

/get/new

Get New

Parameters

Cancel

No parameters

Execute

Responses

Curl

curl -X 'GET' \

Request URL

http://127.0.0.1:8000/get/new

Server response

Code

Details

200

Response body

[{"cveID": "CVE-2023-28461", "vendorProject": "Array Networks ", "product": "Array Networks AG and vxAG ArrayOS Missing Authentication for Critical Function Vulnerability", "vulnerabilityName": "Array Networks AG and vxAG ArrayOS Missing Authentication for Critical Function Vulnerability", "dateAdded": "2024-11-25", "shortDescription": "Array Networks AG and vxAG ArrayOS contain a missing authentication for critical function vulnerability that allows an attacker to read local files and execute code on the SSL VPN gateway.", "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.", "date": "2024-12-16", "knownHansomwareCampaignUse": "Unknown", "notes": "https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_Remote_Code_Execution_Vulnerability_Ag.pdf ; https://nvd.nist.gov/vuln/detail/CVE-2023-28461", "cves": [{"cve": "CVE-306"}]}, {"cveID": "CVE-2024-21287", "vendorProject": "Oracle", "product": "Agile Product Lifecycle Management (PLM)", "vulnerabilityName": "Oracle Agile Product Lifecycle Management (PLM) Incorrect Authorization Vulnerability", "dateAdded": "2024-11-21", "shortDescription": "Oracle Agile Product Lifecycle Management (PLM) contains an incorrect authorization vulnerability in the Process Extension component of the Software Development Kit."}]

GET KNOWN

Known Ransomware CVEs

GET /get/known Get Known

Parameters

No parameters

Execute Clear

Responses

Curl

```
curl -X 'GET' \
  'http://127.0.0.1:8080/get/known' \
  -H 'accept: application/json'
```

Request URL

http://127.0.0.1:8080/get/known

Server response

Code	Details
200	<p>Response body</p> <pre>{ "cveID": "CVE-2024-48711", "vendorProject": "Veeam", "product": "Backup & Replication", "vulnerabilityName": "Veeam Backup and Replication Deserialization Vulnerability", "dataAdded": "2024-10-17", "shortDescription": "Veeam Backup and Replication contains a deserialization vulnerability allowing an unauthenticated user to perform remote code execution.", "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.", "dataDate": "2024-11-07", "knownRansomwareCampaigns": "None", "notes": "https://www.veeam.com/updates ; https://nvd.nist.gov/vuln/detail/CVE-2024-48711", "cwe": ["CWE-502"] }, { "cveID": "CVE-2024-6679", "vendorProject": "Progress", "product": "WhatsUp Gold", "vulnerabilityName": "Progress WhatsUp Gold SQL Injection Vulnerability", "dataAdded": "2024-09-16", "shortDescription": "Progress WhatsUp Gold contains a SQL injection vulnerability that allows an unauthenticated attacker to retrieve the user's encrypted password if the application is configured with only a single user.", "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.", "dataDate": "2024-10-07", "knownRansomwareCampaigns": "None", "notes": "https://www.progress.com/updates ; https://nvd.nist.gov/vuln/detail/CVE-2024-6679" }</pre> <p>Response headers</p> <pre>content-length: 7614 content-type: application/json date: Sun, 01 Dec 2024 19:14:06 GMT server: udcorn</pre>

Responses

Code	Description	Links
200	Successful Response	No links

Media type

application/json

Content-Accept header

SEARCH

Search CVEs

GET /search Search

Parameters

Name Description

query ^{REQUIRED} Keyword to search for

string

(query)

unknown

Execute Clear

Responses

Curl

```
curl -X 'GET' \
  'http://127.0.0.1:8080/search?query=unknown' \
  -H 'accept: application/json'
```

Request URL

http://127.0.0.1:8080/search?query=unknown

Server response

Code	Details
200	<p>Response body</p> <pre>{ "cveID": "CVE-2023-28461", "vendorProject": "Array Networks ", "product": "AG/vxAG ArrayOS", "vulnerabilityName": "Array Networks AG and vxAG ArrayOS Missing Authentication for Critical Function Vulnerability", "dataAdded": "2024-11-20", "shortDescription": "Array Networks AG and vxAG ArrayOS contain a missing authentication for critical function vulnerability that allows an attacker to read local files and execute code on the SSD I/O pathway.", "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.", "dataDate": "2024-12-10", "knownRansomwareCampaigns": "Unknown", "notes": "https://support.arraynetworks.net/pr/001/http://supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_Remote_Code_Execution_Vulnerability_Ag.pdf ; https://nvd.nist.gov/vuln/detail/CVE-2023-28461", "cwe": ["CWE-386"] }, { "cveID": "CVE-2024-21287", "vendorProject": "Oracle", "product": "Oracle Product Lifecycle Management (PLM)", "vulnerabilityName": "Oracle Agile Product Lifecycle Management (PLM) Incorrect Authorization Vulnerability", "dataAdded": "2024-11-21", "shortDescription": "Oracle Agile Product Lifecycle Management (PLM) contains an incorrect authorization vulnerability in the Process Extension component of the Software Development Kit. Successful exploitation of this vulnerability may result in unauthenticated file disclosure.", "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.", "dataDate": "2024-11-21", "knownRansomwareCampaigns": "None", "notes": "https://www.oracle.com/secure/advisories/2024-11-21-plm-remote-code-execution-vulnerability ; https://nvd.nist.gov/vuln/detail/CVE-2024-21287" }</pre> <p>Response headers</p> <pre>content-length: 652338 content-type: application/json date: Sun, 01 Dec 2024 19:55:19 GMT server: udcorn</pre>

Responses