

NVD CVE API :

Overview :

The NVD CVE Dashboard is a web application that fetches CVE data from the official NVD API, stores it in a relational database, and provides a user-friendly interface for exploring vulnerabilities.

It allows security researchers and developers to:

- Synchronize CVEs from NVD into a structured database.
- Query CVEs using filters (year, severity, date, etc.).
- Browse vulnerabilities with a smooth web dashboard.
- View detailed CVE insights with CVSS scores, impacts, and references.

Tech Stack :

- Backend: Python, FastAPI, Psycopg2
- Database: PostgreSQL (Neon Cloud)
- Frontend: HTML, CSS, JavaScript
- Visualization: Chart.js
- Deployment: Uvicorn

System Architecture :

- Database (PostgreSQL)
 - Stores CVEs with metadata and raw JSON.
- Backend (FastAPI)
 - Provides REST endpoints for CVE list & detail.
 - Handles pagination, filtering, and sorting.
- Frontend (Vanilla JS + HTML/CSS)
 - Dashboard to view CVEs.
 - Detail page with expanded info and graphs.

Features :

Backend -

Fetch CVEs from NVD in batches.

Deduplication using CVE ID.

REST API with filtering & sorting.

Paginated results for scalability.

Frontend -

Dashboard (/)

Paginated CVE list.

Filters: CVE ID, Year, Min Score (V2/V3), Last N days.

Sorting by Published or Last Modified date.

Detail Page (/detail.html)

Basic info (CVE ID, description, dates).

CVSS v2 & v3 scores with severity badges.

Attack vector & impact (Confidentiality, Integrity, Availability).

Vulnerable products.

References.

API Documentation :

1. List CVEs

Endpoint: /cves/list

Method: GET

Query Params :

page (int, default=1)

results_per_page (int, default=10)

sort_by (published_date / last_modified)

sort_order (asc / desc)

year (int)
min_score_v3 (float)
min_score_v2 (float)
last_n_days (int)
cve_id (string, partial match)

Response:

```
{
  "page": 1,
  "results_per_page": 10,
  "total_records": 12345,
  "cves": [
    {
      "cve_id": "CVE-2024-1234",
      "year": 2024,
      "published_date": "2024-05-12T14:30:00",
      "last_modified": "2024-06-01T10:00:00",
      "base_score_v3": 7.8,
      "base_score_v2": 6.5,
      "description": "Buffer overflow in XYZ...",
      "raw_json": {}
    }
  ]
}
```

2. CVE Detail

Endpoint: /cves/{cve_id}

Method: GET

Response:

```
{
  "cve_id": "CVE-2024-1234",
  "description": "Buffer overflow in XYZ...",
```

```
"published_date": "2024-05-12T14:30:00",
"last_modified": "2024-06-01T10:00:00",
"base_score_v3": 7.8,
"base_score_v2": 6.5,
"raw_json": {
  "metrics": {
    "cvssMetricV3": [
      {
        "cvssData": {
          "baseScore": 7.8,
          "attackVector": "NETWORK",
          "confidentialityImpact": "HIGH",
          "integrityImpact": "HIGH",
          "availabilityImpact": "HIGH"
        }
      }
    ]
  },
  "references": [
    { "url": "https://vendor.com/security/advisory" }
  ]
}
```

Setup & Deployment :

Prerequisites

Python 3.9+

PostgreSQL (or Neon Cloud DB)

Installation

Clone repo

git clone <repo-url>

cd nvd-dashboard

Install dependencies

`pip install fastapi uvicorn psycpg2-binary`

Run Backend

`python main.py`

Runs at → <http://127.0.0.1:8000>

Access Frontend

Dashboard: <http://127.0.0.1:8000/>

Detail Page: http://127.0.0.1:8000/detail.html?cve_id=CVE-2024-1234

Screenshots :

CVE Security Dashboard

127.0.0.1:8000

Securin Labs

National Vulnerability Database - Security Intelligence Platform

Search CVE ID

Year

Min Score V3

Min Score V2

Last N Days

10

Search

Total Records: 120000

Page 1

| Published | Last Modified | CVE ID | Year | CVSS V3 | CVSS V2 | Description |
|-----------|---------------|-------------------------------|------|---------|---------|--------------------------------------------------------------------|
| 4/4/2014 | 9/25/2025 | CVE-2014-0789 | 2014 | N/A | 5 | Multiple buffer overflows in the OPC Automation 2.0 Server Obj... |
| 4/12/2014 | 9/25/2025 | CVE-2014-0787 | 2014 | N/A | 10 | Stack-based buffer overflow in WellinTech KingSCADA before 3.... |
| 5/1/2014 | 9/25/2025 | CVE-2014-0786 | 2014 | N/A | 7.5 | Ecava IntegraXor before 4.1.4393 allows remote attackers to rea... |
| 3/14/2014 | 9/25/2025 | CVE-2014-0784 | 2014 | N/A | 8.3 | Stack-based buffer overflow in BKBCopyD.exe in Yokogawa CE... |
| 3/14/2014 | 9/25/2025 | CVE-2014-0783 | 2014 | N/A | 9 | Stack-based buffer overflow in BKHODEQ.exe in Yokogawa CEN... |
| 5/16/2014 | 9/25/2025 | CVE-2014-0782 | 2014 | N/A | 8.3 | Stack-based buffer overflow in BKESimMgr.exe in the Expanded... |

27°C

Mostly cloudy

Search

ENG IN

17:50

27-09-2025

CVE Security Dashboard

127.0.0.1:8000

| Published | Last Modified | CVE ID | Year | CVSS V3 | CVSS V2 | Description |
|-----------|---------------|-------------------------------|------|---------|---------|--------------------------------------------------------------------|
| 4/4/2014 | 9/25/2025 | CVE-2014-0789 | 2014 | N/A | 5 | Multiple buffer overflows in the OPC Automation 2.0 Server Obj... |
| 4/12/2014 | 9/25/2025 | CVE-2014-0787 | 2014 | N/A | 10 | Stack-based buffer overflow in WellinTech KingSCADA before 3.... |
| 5/1/2014 | 9/25/2025 | CVE-2014-0786 | 2014 | N/A | 7.5 | Ecava IntegraXor before 4.1.4393 allows remote attackers to rea... |
| 3/14/2014 | 9/25/2025 | CVE-2014-0784 | 2014 | N/A | 8.3 | Stack-based buffer overflow in BKBCopyD.exe in Yokogawa CE... |
| 3/14/2014 | 9/25/2025 | CVE-2014-0783 | 2014 | N/A | 9 | Stack-based buffer overflow in BKHODEQ.exe in Yokogawa CEN... |
| 5/16/2014 | 9/25/2025 | CVE-2014-0782 | 2014 | N/A | 8.3 | Stack-based buffer overflow in BKESimMgr.exe in the Expanded... |
| 3/14/2014 | 9/25/2025 | CVE-2014-0781 | 2014 | N/A | 9.3 | Heap-based buffer overflow in BKLogSvr.exe in Yokogawa CE... |
| 4/25/2014 | 9/25/2025 | CVE-2014-0780 | 2014 | N/A | 7.5 | Directory traversal vulnerability in NTWebServer in InduSoft We... |
| 3/14/2014 | 9/24/2025 | CVE-2014-0779 | 2014 | N/A | 6.8 | The PLC driver in ServerMain.exe in the Kepware KepServerEX 4 ... |
| 4/19/2014 | 9/24/2025 | CVE-2014-0778 | 2014 | N/A | 4.3 | TCPUploader module listens on Port 10651/TCP for incoming c... |

Previous

Page 1

Next

27°C

Mostly cloudy

Search

ENG IN

17:50

27-09-2025

CVE Detail - Security Dashboard

127.0.0.1:8000/detail.html?cve_id=CVE-2014-0789

CVE Security Details

[← Back to Dashboard](#)

Basic Info

| | |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE ID | CVE-2014-0789 |
| Description | Multiple buffer overflows in the OPC Automation 2.0 Server Object ActiveX control in Schneider Electric OPC Factory Server (OFS) TLXCDSUOFS33 3.5 and earlier, TLXCDSTOFS33 3.5 and earlier, TLXCDLUOFS33 3.5 and earlier, TLXCDLTOFS33 3.5 and earlier, and TLXCDLFOFS33 3.5 and earlier allow remote attackers to cause a denial of service via long arguments to unspecified functions. |
| Published Date | 4/4/2014, 3:09:45 PM |
| Last Modified | 9/25/2025, 6:15:36 PM |

CVSS Scores

| | |
|---------------|--------------------------|
| V3 Score | N/A |
| V2 Score | 5 |
| Severity | N/A |
| Attack Vector | AV:N/AC:L/Au:N/CN:N/EA:P |

27°C Mostly cloudy

CVE Detail - Security Dashboard

127.0.0.1:8000/detail.html?cve_id=CVE-2014-0789

Impact

| | |
|-----------------|---------|
| Confidentiality | NONE |
| Integrity | NONE |
| Availability | PARTIAL |

Products & References

| | |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vulnerable Products | 58A9B25F-0A42-4E55-8253-086C8110B46B EDAB2AC4-BF6E-4F66-808D-395DA09A2953 BDB23AE4-FE64-4C13-8703-EBF6A419A149 BE9D2AE1-6047-42C0-9BE5-3DA9C7445F6D FDF237D6-9874-4669-BB85-5047D3D0AFDA |
| References | http://www.schneider-electric.com/corporate/en/support/cybersecurity/viewer-news.page?c_filepath=/templatedata/Content/News/data/en/local/cybersecurity/general_information/2014/03/20140325_vulnerability_disclosure_opc_factory_server.xml http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page https://www.cisa.gov/news-events/ics-advisories/icsa-14-093-01 https://ics-cert.us-cert.gov/advisories/ICSA-14-093-01 http://www.schneider-electric.com/corporate/en/support/cybersecurity/viewer-news.page?c_filepath=/templatedata/Content/News/data/en/local/cybersecurity/general_information/2014/03/20140325_vulnerability_disclosure_opc_factory_server.xml |

27°C Mostly cloudy

Evaluation Checklist :

Logical Approach → Data sync, deduplication, filters.

Code Quality → Clean, modular, well-documented.

Input/Output Screenshots → Provided in repo.

API Docs → Included in README.

UI → Simple, clean, responsive.

Future Enhancements :

Incremental sync (instead of full reload).

CSV/PDF export.

Authentication & role-based dashboards.

Advanced graphs for CVE trends.

Maintained by Viraj Chelamkuri