# CVE API Documentation

## Overview

The CVE API provides access to real vulnerability data from the National Vulnerability Database (NVD) with enhanced analysis including exploit detection, patch availability, and remediation guidance.

## Base URL

http://localhost:3000/api/v1/cves

## Endpoints

### 1. Get CVEs (Paginated with Filters)

GET /api/v1/cves

#### Query Parameters

| Parameter | Type | Description | Example |
| --- | --- | --- | --- |
| page | integer | Page number (default: 1) | ?page=2 |
| limit | integer | Items per page (default: 50) | ?limit=100 |
| severity | string | Filter by severity: critical, high, medium, low | ?severity=critical |
| exploitAvailable | boolean | Filter by exploit availability | ?exploitAvailable=true |
| patchAvailable | boolean | Filter by patch availability | ?patchAvailable=true |
| search | string | Search in CVE ID, description, or search vector | ?search=microsoft |
| sortBy | string | Sort field (default: publishedDate) | ?sortBy=cvss3BaseScore |
| sortOrder | string | Sort order: asc, desc (default: desc) | ?sortOrder=asc |
| minScore | float | Minimum CVSS score | ?minScore=7.0 |
| maxScore | float | Maximum CVSS score | ?maxScore=9.0 |
| dateFrom | date | Published date from (YYYY-MM-DD) | ?dateFrom=2025-01-01 |
| dateTo | date | Published date to (YYYY-MM-DD) | ?dateTo=2025-12-31 |

#### Example Response

{  
 "cves": [  
 {  
 "id": 1,  
 "cveId": "CVE-2025-1234",  
 "description": "Critical buffer overflow vulnerability...",  
 "publishedDate": "2025-07-15T10:00:00.000Z",  
 "lastModifiedDate": "2025-07-15T15:30:00.000Z",  
 "cvss3BaseScore": 9.1,  
 "cvss3Vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H",  
 "cvss2BaseScore": null,  
 "cvss2Vector": null,  
 "exploitAvailable": true,  
 "patchAvailable": true,  
 "source": "NVD",  
 "remediationGuidance": "🔴 CRITICAL: Immediate action required...",  
 "searchVector": "CVE-2025-1234 buffer overflow critical...",  
 "severity": "critical",  
 "cvssScore": 9.1,  
 "createdAt": "2025-07-16T12:00:00.000Z",  
 "updatedAt": "2025-07-16T12:00:00.000Z"  
 }  
 ],  
 "pagination": {  
 "page": 1,  
 "limit": 50,  
 "total": 1000,  
 "pages": 20  
 },  
 "filters": {  
 "severity": "critical",  
 "exploitAvailable": "true"  
 }  
}

### 2. Get Specific CVE

GET /api/v1/cves/:cveId

#### Example

GET /api/v1/cves/CVE-2025-1234

#### Response

{  
 "id": 1,  
 "cveId": "CVE-2025-1234",  
 "description": "Critical buffer overflow vulnerability...",  
 "publishedDate": "2025-07-15T10:00:00.000Z",  
 "cvss3BaseScore": 9.1,  
 "exploitAvailable": true,  
 "patchAvailable": true,  
 "remediationGuidance": "🔴 CRITICAL: Immediate action required. Apply patches within 24 hours.\n• Buffer Overflow: Update to patched version immediately.\n• Monitor vendor security advisories for patches.",  
 "severity": "critical",  
 "cvssScore": 9.1,  
 "cweMappings": [  
 {  
 "cweId": "CWE-119",  
 "cweName": "Improper Restriction of Operations within the Bounds of a Memory Buffer"  
 }  
 ]  
}

### 3. Get CVE Statistics

GET /api/v1/cves/stats/summary

#### Response

{  
 "total": 1000,  
 "bySeverity": {  
 "critical": 58,  
 "high": 230,  
 "medium": 221,  
 "low": 32,  
 "unscored": 459  
 },  
 "exploitAvailable": 45,  
 "patchAvailable": 678,  
 "withGuidance": 950,  
 "recentCves": 247  
}

### 4. Advanced Search

GET /api/v1/cves/search/advanced

#### Query Parameters

| Parameter | Type | Description |
| --- | --- | --- |
| q | string | Search query (required) |
| type | string | Search type: all, exploitable, critical |

#### Examples

GET /api/v1/cves/search/advanced?q=microsoft&type=critical  
GET /api/v1/cves/search/advanced?q=buffer overflow&type=exploitable

## Usage Examples

### Get Critical CVEs with Exploits

curl "http://localhost:3000/api/v1/cves?severity=critical&exploitAvailable=true&limit=10"

### Search for Microsoft Vulnerabilities

curl "http://localhost:3000/api/v1/cves?search=microsoft&sortBy=cvss3BaseScore&sortOrder=desc"

### Get Recent High-Severity CVEs

curl "http://localhost:3000/api/v1/cves?severity=high&dateFrom=2025-07-01&limit=20"

### Get CVE with Full Details

curl "http://localhost:3000/api/v1/cves/CVE-2025-1234"

### Get CVE Statistics

curl "http://localhost:3000/api/v1/cves/stats/summary"

## Response Fields

### CVE Object

| Field | Type | Description |
| --- | --- | --- |
| id | integer | Database ID |
| cveId | string | CVE identifier (e.g., CVE-2025-1234) |
| description | string | Vulnerability description |
| publishedDate | datetime | When CVE was published |
| lastModifiedDate | datetime | When CVE was last modified |
| cvss3BaseScore | float | CVSS v3 base score (0.0-10.0) |
| cvss3Vector | string | CVSS v3 vector string |
| cvss2BaseScore | float | CVSS v2 base score (0.0-10.0) |
| cvss2Vector | string | CVSS v2 vector string |
| exploitAvailable | boolean | Whether exploits are known |
| patchAvailable | boolean | Whether patches are available |
| source | string | Data source (always “NVD”) |
| remediationGuidance | string | Detailed remediation recommendations |
| searchVector | string | Full-text search terms |
| severity | string | Computed severity: critical, high, medium, low, unscored |
| cvssScore | float | Best available CVSS score (v3 preferred) |

## Error Responses

### 404 Not Found

{  
 "error": "CVE not found"  
}

### 400 Bad Request

{  
 "error": "Search query required"  
}

### 500 Internal Server Error

{  
 "error": "Internal server error"  
}

## Rate Limiting

* No rate limiting currently implemented
* Consider implementing rate limiting for production use

## Authentication

* No authentication currently required
* Consider adding API key authentication for production use