Automation Support for CPE Retrieval

Bob Byers
Computer Security Division
Information Technology Laboratory

Harold Owen
Cocoasystems Inc.

September 27, 2019

National Institute of
Standards and Technology
U.S. Department of Commerce

Contents

Introduction

The Official CPE Dictionary, https://nvd.nist.gov/products/cpe/search, is a searchable repository of hardware and software products maintained by the National Vulnerability Database (NVD). NVD offers web services to allow computer applications to access the Official CPE Dictionary and associated vulnerabilities. The purpose of this document is to describe how applications can interact with the CPE web service, version 1.0.

Readers can sample the CPE service by entering this sample URL into any web browser:

```
https://services.nvd.nist.gov/rest/json/cpes/1.0
```

This document is intended for application developers who need to consume the CPE data. It is assumed that the audience is generally familiar with JSON RESTful services. JSON specifies the format of the data returned by the REST service. REST refers to a style of services that allow computers to communicate via HTTP over the Internet.

Section 1 describes the REST parameters that allows you to control and customize which CPE are returned. The service is analogous to the CPE search page, https://nvd.nist.gov/products/cpe/search.

Section 2 describes the response. Most CPE have titles and reference links. Many have associated vulnerabilities. Readers having experience with JSON may also refer to the response schema:

```
https://csrc.nist.gov/schema/cpe/feed/1.0/nvd_cpe_feed_json_1.0.schema
```

The terms product and CPE are used interchangeably throughout this document. CPE means Common Platform Enumeration, version 2.3, a standard for identifying and searching products. For more information, see the naming specification at:

```
https://csrc.nist.gov/publications/detail/nistir/7695/final
```

The CPE 2.3 matching specification is found at:

```
https://csrc.nist.gov/publications/detail/nistir/7696/final
```

Additional services are available for searching vulnerabilities. Readers interested in the vulnerability web services should refer to the guide, *Automation Support for CVE Retrieval.*

Legacy Data Feeds

Historically, CPE information has been available programmatically via data feeds found at https://nvd.nist.gov/products/cpe. Consumers of these legacy feeds are encouraged to migrate *away* from the feeds and use the new services, as the services allow callers to specify query parameters to filter the response.

Note, while the information is similar, the format of the CPE web service response is in JSON and differs from the XML format of the legacy data feeds.

CPE Requests

NVD offers the following REST service to retrieve products.

HTTP Method:	GET
Content Type:	application/json
URL:	https://services.nist.gov/rest/json/cpes/1.0

Parameters	Type	Description	Required?
startIndex	URL query	See Paging Results.	No
resultsPerPage			
modStartDate		CPE modification date range.	
modEndDate			
includeDeprecated		See Deprecated CPE.	
keyword		Free text keyword search.	
cpeMatchString		CPE match string search.	
addOns		Return vulnerabilities.	

All parameters are optional and are intended to limit or *filter* the results. The parameters you use is known collectively as your *search criteria*. The following URL illustrates a request with no search criteria.

```
https://services.nvd.nist.gov/rest/json/cpes/1.0
```

For brevity, the host https://services.nvd.nist.gov/rest/json/ has been omitted from the remaining examples.

Paging Results

By default, the `/cpes` service returns the most recent 20 CPE. The CPE returned can be thought of as a logical *page* of results. You can control which page of results is returned using the startIndex and resultsPerPage parameters. The startIndex parameter determines the first CPE in the response page. The index is zero-based, meaning the first CPE is at index zero.

The resultsPerPage parameter specifies the page size. The actual number of CPE in the page may be fewer depending on how many matched your search criteria. For network considerations, the maximum allowable page size is limited to 5000 CPE.

The total number of results that match your search criteria is indicated in each response. From the total results and your page size, your application can compute the number of requests needed to retrieve all results. See In the examples that follow, a single colon (:) on a line by itself indicates where data has been omitted for clarity.

Total Results, below.

The following URL illustrates how to retrieve the second page of results.

```
cpes/1.0?startIndex=20&resultsPerPage=20
```

Since the default page size is 20, the resultsPerPage is unnecessary in the example.

Retrieving All CPE

Presently NVD contains more than 300,000 product names. If your goal is to fetch all records, then multiple consecutive requests are required. For example, 300+ requests for 1,000 results per page. However, NIST firewall rules in place to prevent denial of service attacks on NVD can thwart your application. To avoid this, it is recommended that your application *sleeps* for several seconds between requests in order that your legitimate requests are not denied.

In addition, applications are discouraged from repeatedly requesting all the records every day. Rather, download all them initially, then use *date range* parameters to retrieve new and recently modified records since your last request. See CPE by Date Range.

CPE by Date Range

Optional modStartDate and modEndDate parameters allow you to retrieve CPE based on when they were added to or modified in the Official Dictionary. Date parameters are in the form:

```
yyyy-MM-dd'T'HH:mm:ss:SSS z
```

It is not necessary to provide both start and end dates if your goal is to retrieve all CPE *after* a certain date, or *up to* a certain date.

The following URL illustrates how to retrieve CPE modified after the start of 2019.

```
cpes/1.0?modStartDate=2019-01-0101T00:00:00:000 UTC-05:00
```

Deprecated CPE

A deprecated CPE is one that previously appeared in the Official CPE Dictionary but has since been replaced by one or more other CPE. CPE are deprecated for various reasons, such as when the original CPE name is discovered to be incorrect, when a more specific CPE name is added, and when a vendor name or product name evolves.

By default, deprecated CPE names are *not* returned by the web service. To include deprecated CPE in the search results, use the includeMatchStringChange=true query parameter.

```
cpes/1.0?includeDeprecated=true
```

Keyword Search

The keyword parameter allows your application to retrieve records where a word or phrase is found in the CPE title or reference links.

```
cpes/1.0?keyword=apple
```

CPE Match String Search

Use the cpeMatchString parameter to further filter CPE results. The cpeMatchString parameter should conform to the CPE 2.3 Matching specification, found at:

```
https://csrc.nist.gov/publications/detail/nistir/7696/final
```

It is beyond the scope of this document to explain the CPE matching syntax. However, a few examples are given here for illustration.

To find CPE names for Microsoft Windows 10, use:

```
cpes/1.0?cpeMatchString=cpe:2.3:o:microsoft:windows_10
```

To find CPE names for version 1511 use:

```
cpes/1.0?cpeMatchString=cpe:2.3:o:microsoft:windows_10:1511
```

To find all CPE names for Microsoft, use:

```
cpes/1.0?cpeMatchString=cpe:2.3:*:microsoft
```

Include Vulnerabilities

Use the optional query parameter addOns=cves to include vulnerabilities associated with the CPE in the response. By default, vulnerabilities are *not* included.

```
cpes/1.0?addOns=cves
```

If this parameter is omitted, then only CPE names are returned.

CPE Response

This section describes the response returned by the CPE service.

In the examples that follow, a single colon (:) on a line by itself indicates where data has been omitted for clarity.

Total Results

The following example illustrates the high-level response to a /cpes service request.

```
{
  "resultsPerPage":20,
  "startIndex":0,
  "totalResults":322194,
  "result": {
    "dataType":"CPE",
    "feedVersion":"1.0",
    "feedTimestamp":"2019-09-16T15:56Z",
    "cpes":[
:
      ]
  }
}
```

Notice that totalResults indicates the total number of CPE that match your search criteria. This is useful in computing the number of requests needed to retrieve all matching pages. See Paging Results.

The result element conforms to nvd_cpe_feed_json_1.0.schema.

The cpes element is the array of CPE (page of results), omitted here.

CPE

At the high-level, each CPE (from the cpes array) can have the following elements.

Element	Description	Required?
deprecated	Indicates whether CPE has been deprecated.	No
cpe23Uri	The CPE name.	Yes
lastModifiedDate	CPE modification date.	Yes
titles	Human-readable CPE titles.	No
refs	Reference links.	No
deprecatedBy	If deprecated=true, one or more CPE that replace this one.	No
vulnerabilities	Optional vulnerabilities associated with this CPE.	No

The following illustrates the JSON structure of the CPE.

```
{
  "deprecated":false,
  "cpe23Uri":"cpe:2.3:a:andy_armstrong:cgi.pm:3.41:*:*:*:*:*:*:*",
  "lastModifiedDate":"2010-12-20T14:34Z",
  "titles":[
:
  ],
  "refs":[
:
  ],
  "deprecatedBy":[
:
  ],
  "vulnerabilities":[
:
  ]
},
```

The cpe23Uri element conforms to the CPE 2.3 Naming specification, found at:

```
https://csrc.nist.gov/publications/detail/nistir/7695/final
```

Note, the CPE Naming specification requires that special charters are preceded by a backslash, and that the JSON syntax of the response requires that backslashes are represented as \\. For instance:

```
"cpe23Uri":"cpe:2.3:a:pcman\\'s_ftp_server_project:pcman\\'s_ftp_server:2.0.7
:*:*:*:*:*:*:*"
```

While the schema requires only the cpe23Uri element, in practice each CPE has a lastModifiedDate.

The remaining sections describe the titles, refs, deprecatedBy, and vulnerabilities elements.

Titles

The titles element contains the human-readable, English title for the CPE. Although it is an array, in practice CPE only have one English title. For example:

```
"titles":[{
  "title":"Tesla Gateway ECU",
  "lang":"en_US"
}]
```

References

The refs element shows one or more Internet links associated with the CPE. Note that NIST categorizes links using the type elements, e.g., Advisory. For example:

```
"refs": [{
  "ref":"https://ics-cert.us-cert.gov/advisories/ICSA-16-341-01",
  "type":"Advisory"
}]
```

Deprecated By

When deprecated=true, the deprecatedBy element shows one or more other CPE that replace this CPE. For example:

```
{
  "deprecated":true,
  "cpe23Uri":"cpe:2.3:a:sun:java_system_messaging_server:6.3:_nil_:x86:
*:*:*:*:*:*",
:
  "deprecatedBy":[
    "cpe:2.3:a:sun:java_system_messaging_server:6.3:-:x86:*:*:*:*:*:*"
  ],
:
}
```

By default, deprecated CPE are not included in the response. See Deprecated CPE, above.

Vulnerabilities

The vulnerabilities element identifies the vulnerabilities associated with the CPE. By default, vulnerabilities are *not* included in the response. See Include Vulnerabilities.


```
"vulnerabilities":[
  "CVE-2001-0606",
  "CVE-2002-1042",
  "CVE-2007-0183",
  "CVE-2002-1042",
  "CVE-2007-0183",
  "CVE-2004-2763"
]
```