Nationwide Endpoint Security

Vulnerability Data Codebook

Table of Contents

[Overview 3](#_Toc395877339)

[Common Platform Enumeration (CPE) 3](#_Toc395877340)

[Vulnerability 3](#_Toc395877341)

[Exposure 4](#_Toc395877342)

[WFN – Well Formed Name 4](#_Toc395877343)

[CVSS – Common Vulnerability Scoring System 5](#_Toc395877344)

[Codebook 6](#_Toc395877345)

[CPE 6](#_Toc395877346)

[PART 6](#_Toc395877347)

[VENDOR 6](#_Toc395877348)

[PRODUCT 6](#_Toc395877349)

[VERSION 6](#_Toc395877350)

[UPDATE 7](#_Toc395877351)

[EDITION 7](#_Toc395877352)

[LANGUAGE 7](#_Toc395877353)

[SW\_EDITION 7](#_Toc395877354)

[TARGET\_SW 7](#_Toc395877355)

[TARGET\_HW 7](#_Toc395877356)

[OTHER 8](#_Toc395877357)

[HIGH 8](#_Toc395877358)

[MEDIUM 8](#_Toc395877359)

[LOW 8](#_Toc395877360)

[SCORES 8](#_Toc395877361)

[REFERENCE 8](#_Toc395877362)

[References 9](#_Toc395877363)

# Overview

## Common Platform Enumeration (CPE)[[1]](#footnote-1)

Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets. CPE does not identify unique instantiations of products on systems, such as the installation of XYZ Visualizer Enterprise Suite 4.2.3 with serial number Q472B987P113. Rather, CPE identifies abstract classes of products, such as XYZ Visualizer Enterprise Suite 4.2.3, XYZ Visualizer Enterprise Suite (all versions), or XYZ Visualizer (all variations).

IT management tools can collect information about installed products, identifying these products using their CPE names, and then use this standardized information to help make fully or partially automated decisions regarding the assets. For example, identifying the presence of XYZ Visualizer Enterprise Suite could trigger a vulnerability management tool to check the system for known vulnerabilities in the software, and also trigger a configuration management tool to verify that the software is configured securely in accordance with the organization's policies. This example illustrates how CPE names can be used as a standardized source of information for enforcing and verifying IT management policies across tools.

The current version of CPE is 2.3. CPE 2.3 is defined through a set of specifications in a stack-based model, where capabilities are based on simpler, more narrowly defined elements that are specified lower in the stack. This design opens opportunities for innovation, as novel capabilities can be defined by combining only the needed elements, and the impacts of change can be better compartmentalized and managed.

## Vulnerability[[2]](#footnote-2)

An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network.

CVE considers a mistake a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system (this excludes entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system).

For CVE, a vulnerability is a state in a computing system (or set of systems) that either:

* allows an attacker to execute commands as another user
* allows an attacker to access data that is contrary to the specified access restrictions for that data
* allows an attacker to pose as another entity
* allows an attacker to conduct a denial of service

Examples of vulnerabilities include:

* phf (remote command execution as user "nobody")
* rpc.ttdbserverd (remote command execution as root)
* world-writeable password file (modification of system-critical data)
* default password (remote command execution or other access)
* denial of service problems that allow an attacker to cause a Blue Screen of Death
* smurf (denial of service by flooding a network)

## Exposure[[3]](#footnote-3)

An information security "exposure" is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

CVE considers a configuration issue or a mistake an exposure if it does not directly allow compromise but could be an important component of a successful attack, and is a violation of a reasonable security policy.

An "exposure" describes a state in a computing system (or set of systems) that is not a vulnerability, but either:

* allows an attacker to conduct information gathering activities
* allows an attacker to hide activities
* includes a capability that behaves as expected, but can be easily compromised
* is a primary point of entry that an attacker may attempt to use to gain access to the system or data
* is considered a problem according to some reasonable security policy

Examples of exposures include:

* running services such as finger (useful for information gathering, though it works as advertised)
* inappropriate settings for Windows NT auditing policies (where "inappropriate" is enterprise-specific)
* running services that are common attack points (e.g., HTTP, FTP, or SMTP)
* use of applications or services that can be successfully attacked by brute force methods (e.g., use of trivially broken encryption, or a small key space)

## WFN – Well Formed Name[[4]](#footnote-4)

A WFN is an unordered set of attribute-value pairs that collectively (a) describe or identify a software application, operating system, or hardware device, and (b) satisfy the criteria specified in Section 5.2. Unordered means that there is no prescribed order for the attribute-value pairs, and there is no specified relationship (hierarchical, set-theoretic, or otherwise) among attributes or attribute-value pairs.

The WFN is a logical construct only. The WFN is not intended to be a data format, encoding, or any other kind of machine-readable representation for machine interchange and processing. Rather, it is a conceptual data structure—an abstract canonical form—used to clearly and unambiguously specify desired implementations and behaviors. There is no requirement that CPE-conformant tools create or manipulate WFN-like data structures internally to their implementations. Section 6 describes procedures for binding WFNs to machine-readable representations for interchange and processing.

## CVSS – Common Vulnerability Scoring System[[5]](#footnote-5)

CVSS stands for The Common Vulnerability Scoring System and is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response. It solves the problem of multiple, incompatible scoring systems and is usable and understandable by anyone.

Scoring is the process of combining all the metric values according to specific formulas. Base Scoring is computed by the vendor or originator with the intention of being published and once set, is not expected to change. It is computed from the big three confidentiality, integrity and availability. This is the foundation which is modified by the Temporal and Environmental metrics. The base score has the largest bearing on the final score and represents vulnerability severity.

Temporal Scoring is also computed by vendors and coordinators for publication, and modifies the Base score. It allows for the introduction of mitigating factors to reduce the score of a vulnerability and is designed to be re-evaluated at specific intervals as a vulnerability ages. The temporal score represents vulnerability urgency at specific points in time.

Environmental Scoring is optionally computed by end-user organizations and adjusts combined Base-Temporal score. This should be considered the FINAL score and represents a snapshot in time, tailored to a specific environment. User organizations should use this to prioritize responses within their own environments.

# Codebook

|  |  |  |
| --- | --- | --- |
| CPE | | Column A |
| Description |  | |
| Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise’s computing assets.  This type of binding is referred to as a Uniform Resource Identifier (URI) binding. There is another binding type refered to as Formatted String Binding whose syntax is somewhat different and is distinguished by the string starting with cpe:2.3  This column contains the all CPE’s in URI form taken from NIST located at <http://nvd.nist.gov/cpe.cfm>. There are approximately 95 thousand applications contained in the NIST Dataset. | | |

|  |  |  |
| --- | --- | --- |
| PART | | Column B |
| Description |  | |
| PART identifies the type of Item the CPE refers to.   * The value “a”, when the WFN is for a class of applications. * The value “o”, when the WFN is for a class of operating systems. * The value “h”, when the WFN is for a class of hardware devices. | | |

|  |  |  |
| --- | --- | --- |
| VENDOR | | Column C |
| Description |  | |
| Values for this attribute SHOULD describe or identify the person or organization that manufactured or created the product. | | |

|  |  |  |
| --- | --- | --- |
| PRODUCT | | Column D |
| Description |  | |
| Values for this attribute SHOULD describe or identify the most common and recognizable title or name of the product. | | |

|  |  |  |
| --- | --- | --- |
| VERSION | | Column E |
| Description |  | |
| Values for this attribute SHOULD be vendor-specific alphanumeric strings characterizing the particular release version of the product. Version information SHOULD be copied directly (with escaping of printable non-alphanumeric characters as required) from discoverable data and SHOULD NOT be truncated or otherwise modified. | | |

|  |  |  |
| --- | --- | --- |
| UPDATE | | Column F |
| Description |  | |
| Values for this attribute SHOULD be vendor-specific alphanumeric strings characterizing the particular update, service pack, or point release of the product. | | |

|  |  |  |
| --- | --- | --- |
| EDITION | | Column G |
| Description |  | |
| The edition attribute is considered deprecated in this specification, and it SHOULD be assigned the logical value ANY except where required for backward compatibility with version 2.2 of the CPE specification. This attribute is referred to as the “legacy edition” attribute.  If this attribute is used, values for this attribute SHOULD capture edition-related terms applied by the vendor to the product. | | |

|  |  |  |
| --- | --- | --- |
| LANGUAGE | | Column H |
| Description |  | |
| Values for this attribute SHALL be valid language tags as defined by [RFC5646], and SHOULD be used to define the language supported in the user interface of the product being described. Although any valid language tag MAY be used, only tags containing language and region codes SHOULD be used. | | |

|  |  |  |
| --- | --- | --- |
| SW\_EDITION | | Column I |
| Description |  | |
| Values for this attribute SHOULD characterize how the product is tailored to a particular market or class of end users.. | | |

|  |  |  |
| --- | --- | --- |
| TARGET\_SW | | Column J |
| Description |  | |
| Values for this attribute SHOULD characterize the software computing environment within which the product operates. | | |

|  |  |  |
| --- | --- | --- |
| TARGET\_HW | | Column K |
| Description |  | |
| Values for this attribute SHOULD characterize the instruction set architecture (e.g., x86) on which the product being described or identified by the WFN operates. Bytecode-intermediate languages, such as Java bytecode for the Java Virtual Machine or Microsoft Common Intermediate Language for the Common Language Runtime virtual machine, SHALL be considered instruction set architectures. | | |

|  |  |  |
| --- | --- | --- |
| OTHER | | Column L |
| Description |  | |
| Values for this attribute SHOULD capture any other general descriptive or identifying information which is vendor- or product-specific and which does not logically fit in any other attribute value. Values SHOULD NOT be used for storing instance-specific data (e.g., globally-unique identifiers or Internet Protocol addresses). | | |

|  |  |  |
| --- | --- | --- |
| HIGH | | Column M |
| Description |  | |
| The HIGH field is a count of the number of CVEs with a CVSS score of 7 or higher that apply to this CPE. If none meet this requirement a “-“ is inserted. If there are no CVEs that apply to this CPE then the HIGH, MEDIUM, LOW and SCORES field will be blank or null. | | |

|  |  |  |
| --- | --- | --- |
| MEDIUM | | Column N |
| Description |  | |
| The MEDIUM is a count of the number of CVEs with a CVSS score between 4 and 7 that apply to this CPE . If none meet this requirement a “-“ is inserted. If there are no CVEs that apply to this CPE then the HIGH, MEDIUM, LOW and SCORES field will be blank or null. | | |

|  |  |  |
| --- | --- | --- |
| LOW | | Column O |
| Description |  | |
| The LOW is a count of the number of CVEs with a CVSS score less then 4 that apply to this CPE. If none meet this requirement a “-“ is inserted. If there are no CVEs that apply to this CPE then the HIGH, MEDIUM, LOW and SCORES field will be blank or null. | | |

|  |  |  |
| --- | --- | --- |
| SCORES | | Column P |
| Description |  | |
| This is an aggregate of all of the CVSS scores that apply to this CVE. They are a colon “:” separated list of score 1.0-10. 0. | | |

|  |  |  |
| --- | --- | --- |
| REFERENCE | | Column Q |
| Description |  | |
| If there are CVEs that apply this CPE then a link will be provided referencing the source material on the NVD website. This link will provide additional details regarding the vulnerabilities that are available. | | |

# References

<http://scap.nist.gov/specifications/cpe/>

<http://nvd.nist.gov/home.cfm>

<http://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf>

<http://www.first.org/cvss/faq>

1. This text taken from the CPE website hosted on nist http://scap.nist.gov/specifications/cpe/ [↑](#footnote-ref-1)
2. This text taken from the CVE website hosted on mitr http://cve.mitre.org/about/terminology.html [↑](#footnote-ref-2)
3. This text taken from the CVE website hosted on mitr http://cve.mitre.org/about/terminology.html [↑](#footnote-ref-3)
4. This text taken from the CPE naming document hosted on NIST http://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf [↑](#footnote-ref-4)
5. Taken from CVSS data hosted on first.org http://www.first.org/cvss/faq [↑](#footnote-ref-5)