Common Platform Enumeration — CPE™

A Structured Naming Scheme for IT Systems, Platforms, and Packages

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 can be used as a source of information for enforcing and verifying IT management policies relating to these assets, such as vulnerability, configuration, and remediation policies. IT management tools can collect information about installed products, identify products using their CPE names, and use this standardized information to help make fully or partially automated decisions regarding the assets.

Challenge

Secure information systems depend on reliable, cost-effective Software Asset Management practices that support security assessment. IT managers need highly reliable and automatable software inventory processes that provide accurate, up-to-the-minute details about the operating systems, software applications and hardware devices that are installed and available for use. Once armed with this data, IT managers can identify risks and vulnerabilities, and make timely decisions about what to install, patch or disable.

Specification languages exist such as Common Vulnerabilities and Exposures (CVE®) for describing vulnerabilities, Open Vulnerability and Assessment Language (OVAL®) for testing system state, and Extensible Configuration Checklist Description Format (XCCDF) for expressing security checklists.

What these languages all have in common, however, is a need to refer to IT products and platforms in a standardized way that is suitable for machine interpretation and processing. CPE satisfies that need.

Solution

Developed specifically to work with specification languages, CPE provides:

- A standard machine-readable format for encoding names of IT products and platforms.
- A set of procedures for comparing names.
- A language for constructing "applicability statements" that combine CPE names with simple logical operators.
- A standard notion of a CPE Dictionary.

CPE in the Enterprise

An authoritative CPE Dictionary is currently maintained by the National Institute of Standards and Technology (NIST) as part of its U.S. National Vulnerability Database (NVD). NIST also hosts the current official version of the CPE Specification documents, Version 2.3.

In addition, CPE is one of the existing open standards used by NIST in its Security Content Automation Protocol (SCAP) program, which combines "a suite of tools to help automate vulnerability management and evaluate compliance with federal information technology security requirements." Numerous products have been validated by NIST as conforming to the CPE component of SCAP.

CPE Dictionary

Hosted by NIST, the "Official CPE Dictionary" currently includes 43,000+ unique CPE Names. Its main purposes are to:

- Provide a canonical source for all known CPE Names.
- Bind descriptive metadata (such as a title and notes) to a CPE Name.
- Bind diagnostic tests (such as an automated check to determine if a given platform matches the name) to a CPE Name.

CPE™

cpe.mitre.org

The MITRE Corporation maintains CPE's public Web site presence and provides impartial technical guidance to the CPE Community throughout the process to ensure CPE serves the public interest.

202 Burlington Road, Bedford, MA 01730-1420
www.mitre.org
MITRE

Since CPE Names contain the names and versions of software and hardware products, vendor participation is critical to ensuring that product names are accurately represented in the CPE Dictionary. Join the many vendors that are already using CPE to help validate the names of their products by contacting us at cpe@mitre.org.

CPE Specification

CPE Version 2.3 includes four separate specifications organized in a stack, with each building on those that precede it. Hosted by NIST, the CPE 2.3 Specifications focus on the following:

Naming

The CPE 2.3 Naming Specification defines standardized methods for assigning names to IT product classes using an abstract logical construction known as a well-formed CPE name (WFN). The CPE Naming Specification defines procedures for binding WFNs to machine-readable encodings, as well as unbinding those encodings back to WFNs. Backward compatibility is also maintained with CPE 2.2's Uniform Resource Identifier (URI) binding method (e.g., the URI binding representation of the WFN example above is: "cpe:/a:microsoft:internet_explorer:8.0.6001:beta").

Example WFN for Microsoft Internet Explorer 8.0.6001 Beta:
wfn: [part="a",vendor="microsoft",product="internet_explorer", version="8\.0\.6001", update="beta"]

The Official CPE Dictionary contains an authoritative enumeration of CPE names in URI binding. The WFN binding defined in CPE 2.3 is a formatted string binding that has a somewhat different syntax than the URI binding and supports additional product attributes. With the formatted string binding, the WFN above can be represented by: "cpe:2.3:a:microsoft:internet_explorer:8.0.6001:beta:*:*:*:*:*:*" The WFN concept and the bindings defined by the CPE Naming Specification are the fundamental building blocks at the core of all CPE functionality.

Matching

The CPE 2.3 Name Matching Specification defines a method for conducting a one-to-one comparison of a source CPE name to a target CPE name. By logically comparing CPE names as sets of values, CPE Name Matching methods can determine if common set relations hold. For example, CPE Name Matching can determine if the source and target names are equal, if one of the names is a subset of the other, or if the names are disjoint. This is a powerful and flexible way of performing product comparisons in a standardized, automated manner. CPE Name Matching is also used by other CPE specifications to conduct more complex tasks, such as searching for product names in CPE dictionaries and performing complex comparisons of sets of product versions—for example, determining if a system is running a particular operating system version, running two particular applications, and not running a third particular application.

Dictionary

The CPE 2.3 Dictionary Specification defines a standardized method for creating and managing public and/or private CPE dictionaries (e.g., the public Official CPE Dictionary). A "dictionary" is a repository of CPE names and metadata associated with the names. Each CPE name in the dictionary identifies a single class of IT product in the world, with the word "class" signifying that the object identified is not a physical instantiation of a product on a system, but rather the abstract model of that product. Although organizations may use a CPE name to represent either a single product class or a set of multiple product classes, a CPE dictionary stores only bound forms of well-formed CPE names that identify a single product class, not a set of product classes.

Applicability Language

The CPE 2.3 Applicability Language Specification defines a standardized way to describe IT platforms by forming complex logical expressions out of individual CPE names and references to checks. The CPE Applicability Language Data Model builds on top of the other CPE specifications to provide the functionality required to allow CPE users to construct complex groupings of CPE names to describe IT platforms. These groupings are referred to as applicability statements because they are used to designate to which platforms particular guidance, policies, etc., apply.

Join the Community

Members of the information technology and information security communities are invited to join the CPE Email Discussion List at http://cpe.mitre.org/community/discussion_list.html.