Common Configuration Enumeration — CCE™
Standardized Identifiers for Security Configuration Issues and Exposures

MITRE

CCE PROVIDES UNIQUE IDENTIFIERS to security-related system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools.

For example, CCE-IDs are used for mappings between configuration best-practice documents such as the CIS Benchmarks, DISA STIGs, Unified Compliance Framework, etc. CCE-IDs are included in the 2008 Microsoft Windows Server Security Guide and 2007 Microsoft Office Security Guide, and are the main identifiers used for the settings in the U.S. Federal Desktop Core Configuration (FDCC) data file downloads.

CCE is also one of the community standards that helps enable the National Institute of Standards and Technology (NIST's) Security Content Automation Protocol (SCAP).

Why CCE

When dealing with information from multiple sources, use of consistent identifiers can improve data correlation; enable interoperability; foster automation; and ease the gathering of metrics for use in situation awareness, IT security audits, and regulatory compliance. For example, Common Vulnerabilities and Exposures (CVE®) provides this capability for information security vulnerabilities.

Similar to the CVE effort, CCE assigns a unique, common identifier to a particular security-related configuration issue. CCE identifiers are associated with configuration statements that express the way humans name and discuss their intentions when configuring computer systems (see the CCE Editorial Policies on the CCE Web site for detailed content decisions). In this way, the use of CCE Identifiers (CCE-IDs) as tags provide a bridge between natural language, prose-based configuration guidance documents and machine-readable or executable capabilities such as configuration audit tools.

Each entry on the CCE List contains the following five attributes:

- CCE Identifier Number - current version is "CCE-3243-3"
- Description - a humanly understandable description of the configuration issue
- Conceptual Parameters - parameters that would need to be specified in order to implement a CCE on a system
- Associated Technical Mechanisms - for any given configuration issue there may be one or more ways to implement the desired result
- References - pointers to the specific sections of the documents or tools in which the configuration issue is described in detail

Currently, CCE is focused solely on software-based configurations. Recommendations for hardware and/or physical configurations are not supported. Refer to the CCE List on the CCE Web site for more information.

CCE Working Group

CCE is industry-endorsed through the CCE Working Group, which includes members from major operating systems vendors, commercial information security tool vendors, academia, government agencies, and research institutions. View current members on the CCE Working Group page on the CCE Web site.

If you or your organization would like to be considered for possible involvement in this working group, please contact us at cce@mitre.org.

cce.mitre.org

CCE Entry Attributes

Entries in the CCE List contain the following five attributes:

CCE Identifier	Like CVE, CCE assigns identifier tags to each commonly recognized configuration issue. These identifiers are intended to be unique tags or keys, not descriptive names. By way of a loose analogy, CCE-IDs are like scientific names for animals, providing a precise identifier for a species that is agreed upon by the technical community but which may have little or no meaning in common language usage.
Description	CCE entries contain a humanly understandable description of the configuration issue. This description is intended to describe the generic issue. In particular, it is not intended to make an assertion as to what particular configuration should or should not be made. For example, a valid CCE description might be "The minimum password length should be set appropriately". CCE makes no assertion whether the minimum password length should be 8, 10, or 14. It only describes the generic and non-qualified issue of minimum password length.
Conceptual Parameters	CCE entries contain a list of conceptual parameters that would be needed to be specified in order to implement a CCE on a system. For example, for the CCE associated with "The startup type of the Telnet service should be correct" (for Windows) the conceptual parameters would be Automatic, Manual, and Disabled. CCE entries distinguish between such humanly understandable conceptual parameters and machine understandable parameters such as the specific registry key values that might be associated with the conceptual notions of "Automatic", "Manual", and "Disabled".
Associated Technical Mechanisms	For any given configuration issue there may be more than one way to implement the desired result. For example, in Windows the issue of "The Autoplay feature should be set correctly for all drives" issue can be set either with a direct registry key edit or by way of a Group Policy Object if the system participates in an Active Directory domain. And in most forms of UNIX and Linux, the issue of "The FTP service should be enabled or disabled as appropriate" can be achieved in multiple ways. One way to understand the distinction between the Description and its corresponding set of Technical Mechanisms is that the former describes a goal and the latter describes a set of ways to achieve that goal.
References	Each CCE entry has a set of references from published configuration guidance documents such as the NSA Security Guides, the Center for Internet Security Benchmarks, and DISA STIGS that point to the specific sections of the documents or tools in which the configuration issue is described in more detail. These references (1) provide a logical linkage to more detailed information, (2) validate the need for a CCE entry for any given configuration issue, and (3) validate that the CCE entry is described at a level of abstraction that is used and accepted within the community.

Member of

http://measurablesecurity.mitre.org

Making
Security
Measurable™

Learn More - http://cce.mitre.org