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

Special Publication 800-51
Revision 1 (Draft)

Guide to Using Vulnerability Naming Schemes (Draft)

Recommendations of the National Institute of Standards and Technology

David Waltermire
Karen Scarfone

NIST Special Publication 800-51
Revision 1 (Draft)

Guide to Using Vulnerability Naming Schemes (Draft)

Recommendations of the National Institute of Standards and Technology

David Waltermire
Karen Scarfone

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

November 2010



U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-51 Revision 1 (Draft)
Natl. Inst. Stand. Technol. Spec. Publ. 800-51 rev. 1 (Draft), 13 pages (Nov. 2010)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgments

The authors, David Waltermire of the National Institute of Standards and Technology (NIST) and Karen Scarfone of G2, Inc. wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content, particularly John Banghart, Tim Grance, Chris Johnson, and Murugiah Souppaya of NIST. The authors would also like to acknowledge Peter Mell and Tim Grance of NIST for authoring the original version of this publication, which was released in 2002.

Trademark Information

CVE is a registered trademark, and CCE and CPE are trademarks, of The MITRE Corporation.

All other names are registered trademarks or trademarks of their respective companies.

Table of Contents

1. Introduction 1

1.1 Authority 1
1.2 Purpose and Scope 1
1.3 Audience 1
1.4 Document Structure 1

2. Overview of Vulnerability Naming Schemes 2

2.1 Common Vulnerabilities and Exposures (CVE) 2
2.2 Common Configuration Enumeration (CCE) 5 3

3. Recommendations for End-User Organizations 4

3.1 Product and Service Selection and Design 4
3.2 Vulnerability Communications and Reporting 4

4. Recommendations for Software Developers and Service Providers 6

4.1 Name Creation 6
4.2 Name Use 6

Appendix A— Acronyms and Abbreviations A-1

Appendix B— References B-1

List of Figures

Figure 1. Example CVE Entry 2

Figure 2. Example CCE Entry 3

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

The purpose of this document is to provide recommendations for using vulnerability naming schemes. The document covers two schemes: CVE and CCE. The document gives an introduction to both schemes and makes recommendations for end-user organizations on using the names produced by these schemes. The document also presents recommendations for software and service vendors on how they should use vulnerability names and naming schemes in their product and service offerings.

1.3 Audience

The intended audience for this document is individuals who have responsibilities related to vulnerability management.

1.4 Document Structure

The remainder of this document is organized into the following major sections and appendices:

- Section 2 provides an overview of CVE and CCE.
- Section 3 gives recommendations to end-user organizations on using CVE and CCE.
- Section 4 makes recommendations for how IT product and service vendors should adopt CVE and CCE within their product and service offerings.
- Appendix A defines acronyms and abbreviations for the document.
- Appendix B lists related resources.

2. Overview of Vulnerability Naming Schemes

A *vulnerability naming scheme* is a systematic method for creating and maintaining a standardized dictionary of common names for a set of vulnerabilities in IT systems, such as software flaws in an operating system or security configuration issues in an application. The naming scheme ensures that each vulnerability entered into the dictionary has a unique name. Using standardized vulnerability naming schemes supports interoperability. Organizations typically have many tools for system security management that reference vulnerabilities—for example, vulnerability and patch management software, vulnerability assessment tools, antivirus software, and intrusion detection systems. If these tools do not use standardized names for vulnerabilities, it may not be clear that multiple tools are referencing the same vulnerabilities in their reports, and it may take extra time and resources to resolve these discrepancies and correlate the information. This lack of interoperability can cause delays and inconsistencies in security assessment, reporting, decision-making, and vulnerability remediation, as well as hampering communications both within organizations and between organizations. Use of standardized names also helps minimize confusion regarding which problem is being addressed, such as which vulnerabilities a new patch mitigates. This helps organizations to quickly identify the information they need, such as remediation information, when a new problem arises.

This publication provides information and recommendations related to the two most widely used vulnerability naming schemes: Common Vulnerabilities and Exposures (CVE), and Common Configuration Enumeration (CCE). Both are described in detail below.

2.1 Common Vulnerabilities and Exposures (CVE)

The CVE vulnerability naming scheme is for a dictionary of unique, common names for publicly known software flaws. CVE provides the following:

- A comprehensive list of publicly known software flaws
- A globally unique name to identify each vulnerability
- A basis for discussing priorities and risks of vulnerabilities
- A way for a user of disparate products and services to integrate vulnerability information

A CVE vulnerability entry consists of a unique identifier number, a short description of the vulnerability, and references to public advisories on the vulnerability. Figure 1 shows an example.

CVE ID:	CVE-2000-0001
Description:	RealMedia server allows remote attackers to cause a denial of service via a long ramgen request.
References:	BUGTRAQ: 19991222 RealMedia Server 5.0 Crasher (rmscrash.c) BID:888 URL:http://www.securityfocus.com/bid/888 XF:realserver-ramgen-dos

Figure 1. Example CVE Entry

Working with researchers, The MITRE Corporation assigns CVE IDs to publicly known vulnerabilities in commercial and open source software. General information on CVE is available at http://cve.mitre.org/. The National Vulnerability Database (NVD), which is maintained by NIST, provides several ways of

accessing CVE entries. NVD offers CVE search capabilities, as well as a variety of XML and RSS data feeds with CVE entries and supplemental information to support security automation technologies. NVD is publicly available at http://nvd.nist.gov/.

The MITRE Corporation maintains information on the use of CVE. Vendors that include CVE identifiers in their security advisories are listed at http://cve.mitre.org/compatible/alerts_announcements.html. Products and services that have been reviewed and evaluated by the MITRE Corporation and determined to be "CVE-compatible", which means that they meet a set of CVE requirements, are listed at http://cve.mitre.org/compatible/compatible.html.

2.2 Common Configuration Enumeration (CCE) 5

The CCE 5 vulnerability naming scheme is for a dictionary of names for software security configuration settings. Each type of security-related configuration issue is assigned a unique identifier to facilitate fast and accurate correlation of configuration data across multiple information sources and products.

There are five attributes in a CCE entry: a unique identifier number, a description of the configuration issue, logical parameters of the CCE, the associated technical mechanisms related to the CCE, and references to additional sources of information. Figure 2 provides an example of these attributes for a CCE 5 entry for Windows XP.

CCE ID:	CCE-3108-8
Description:	The correct service permissions for the Telnet service should be assigned.
Parameters:	(1) set of accounts (2) list of permissions
Technical Mechanisms:	(1) set via Security Templates (2) defined by Group Policy
References:	Listed at http://cce.mitre.org/lists/cce_list.html

Figure 2. Example CCE Entry

The MITRE Corporation maintains and publishes the lists of CCE names. The lists, and additional information on CCE, are available at http://cce.mitre.org/.

3. Recommendations for End-User Organizations

This section provides recommendations for end-user organizations on how they should take advantage of the CVE and CCE specifications to improve their system security management. For all recommendations in this section involving an organization using CVE and CCE names, the organization should use the authoritative names; locations for downloading these are listed in Section 2.

Some of the recommendations in this section involve the Common Platform Enumeration (CPE) version 2.2 specification. CPE provides standardized, consistent names for referring to operating systems, hardware, and applications. CPE names are often used in conjunction with CVE and CCE names. Each CVE name and CCE name is related to one or more IT components, which can be expressed using CPE names. For example, a particular software flaw (identified by a CVE name) may affect seven products (identified by their CPE names). Using CPE names with CVE and CCE names further supports interoperability and standardization across products and services. The official CPE dictionary is available at http://nvd.nist.gov/cpe.cfm.

3.1 Product and Service Selection and Design

1. When evaluating IT products and services that use vulnerability names, such as for possible acquisition, organizations should take into consideration the products and services' support for CVE and/or CCE (as appropriate). Most organizations use a variety of products and services to detect, track, and mitigate vulnerabilities. Using standardized vulnerability names across products and services makes it much easier and faster to correlate information and to aggregate data from many disparate sources into a unified interface, such as a security dashboard.

2. Organizations developing their own custom security software that will use vulnerability names should ensure that the software uses authoritative CVE and/or CCE names, as appropriate, and uses CPE names with them when indicating which IT products the CVE and CCE names apply to. Using CVE, CCE, and CPE names supports interoperability with other software and services.

3.2 Vulnerability Communications and Reporting

1. Organizations should use authoritative CVE and CCE names in their internal vulnerability assessment and reporting, including assessment reports, notifications to system owners of detected vulnerabilities, and alerts identifying the vulnerabilities being targeted by active exploits. Use of CVE and CCE names will help to minimize confusion regarding which vulnerability is being referenced and whether a particular vulnerability has been mitigated. Organizations should also use CPE names when indicating which IT products the vulnerabilities apply to.

2. Organizations should use authoritative CVE and CCE names in their external vulnerability communications, as well as the CPE names for the IT products that the vulnerabilities apply to. For example, communications to incident response teams should reference, when known, the CVE or CCE names of the vulnerabilities that are being exploited and the CPE names of the products that are being exploited. This ensures that incident communications precisely identify relevant vulnerabilities and affected products, enable correlation and integration of reports, and enable correlation with supplemental information residing in other data repositories. Another example is that organizations should use CVE and CCE names when communicating with vendors that support CVE and CCE names. Suppose that a vendor-supplied patch that purports to fix a vulnerability is defective; a statement to the vendor that a given CVE vulnerability remains after applying the patch conveys important information clearly and succinctly. Communications with vendors of scanning tools regarding false positives or false negatives will be clearer if the

offending vulnerability is labeled by CVE or CCE name.

3. As recommended in NIST SP 800-117 Revision 1, organizations should encourage security software vendors to incorporate support for CVE and CCE into their products, as well as encourage all software vendors to include authoritative CVE and CCE names in their product security advisories and other security-related documentation and communications, as well as to reference the CPE names for their products.

4. Recommendations for Software Developers and Service Providers

This section makes recommendations for how software developers and service providers should take advantage of CVE and CCE's capabilities. This improves interoperability, thus increasing the efficiency of security management and improving the security of systems. Also, as described in the introduction to Section 3, using CPE names when indicating which products CVE and CCE names apply to further supports interoperability and standardization.

4.1 Name Creation

1. Software developers should participate in the CVE issuance processes to help ensure that CVEs provide the necessary information and are created in a timely manner, such as while planning a public vulnerability announcement or immediately after a vulnerability has been publicly announced. For more information on the CVE issuance process, see http://cve.mitre.org/cve/identifiers/index.html or contact cve@mitre.org.

2. Authors of CVE names should reference applicable vendor patch identification whenever possible.

3. Software developers are encouraged to work with the MITRE Corporation to establish unique CCE identifiers for their products' security configuration settings. Basic information on this is available at http://cce.mitre.org/lists/creation_process.html. Software developers should contact the CCE Content Team at cce@mitre.org for more information on the process.

4.2 Name Use

1. Software developers and service providers should incorporate support for CVE and CCE into their products and services that reference publicly known software vulnerabilities. Also, CPE names should be used when indicating which products the CVE and CCE names apply to.

2. Software developers and service providers should incorporate the appropriate authoritative CVE and/or CCE names in their security advisories and other vulnerability-related documentation and communications, as well as the CPE names that indicate which products the CVE and/or CCE names apply to. Using CVE, CCE, and CPE names supports the use of standardized security automation technologies, which rely on common vulnerability and product names, and ensures clarity when referencing a given vulnerability.

Appendix A—Acronyms and Abbreviations

Selected acronyms and abbreviations used in the publication are defined below.

CCE	Common Configuration Enumeration
CVE	Common Vulnerabilities and Exposures
FISMA	Federal Information Security Management Act
IT	Information Technology
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NVD	National Vulnerability Database
OMB	Office of Management and Budget
RSS	Really Simple Syndication
SP	Special Publication
URL	Uniform Resource Locator
XML	Extensible Markup Language

Appendix B—References

This appendix lists references with additional information related to vulnerability naming schemes.

Resource	URL
CCE	http://cce.mitre.org/
CCE List	http://cce.mitre.org/lists/cce_list.html
CPE	http://cpe.mitre.org/
CPE dictionary	http://nvd.nist.gov/cpe.cfm
CVE	http://cve.mitre.org/
CVE-compatible products and services	http://cve.mitre.org/compatible/compatible.html
CVE identifier use in security advisories	http://cve.mitre.org/compatible/alerts_announcements.html
NVD	http://nvd.nist.gov/