Guidelines to Federal Organizations on Use of the CVE Vulnerability Naming Scheme Within its Acquired Products and Information Technology Security Procedures

Recommendations of the
National Institute of Standards and Technology (NIST)

Authors: Peter Mell and Tim Grance

Purpose

This document provides guidelines for federal organizations' acquisition and use of security-related information technology (IT) products and services. NIST's advice is provided in the context of larger recommendations regarding security assurance (see NIST Special Publication 800-23, http://csrc.nist.gov).

This document has been developed by NIST in furtherance of its statutory responsibilities (under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996, specifically 15 U.S.C. 278 g-3 (a)(5)). This is not a guideline within the meaning of (15 U.S.C. 278 g-3 (a)(3)).

These guidelines are for use by federal organizations which process sensitive information. They are consistent with the requirements of Office of Management and Budget (OMB) Circular A-130, Appendix III.

The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis. It is not subject to copyright.

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

Background

The Common Vulnerabilities and Exposures (CVE) vulnerability naming scheme is a dictionary of common names for publicly known IT system vulnerabilities. It is an emerging industry standard that has achieved wide acceptance by the security industry and a number of government organizations. Technical vulnerability experts from 31 industry, academia, and government organizations vote on the common names. CVE provides the computer security community with:

1. a comprehensive list of publicly known vulnerabilities,
2. an analysis of the authenticity of newly published vulnerabilities, and
3. a unique name to be used for each vulnerability.

General CVE information is available at http://cve.mitre.org. The vulnerabilities listed in CVE can be viewed using the NIST ICAT vulnerability index at http://icat.nist.gov.

Guidelines

1. Federal departments and agencies should give substantial consideration to the acquisition and use of security-related IT products and services that are compatible with the CVE vulnerability naming scheme.

Most federal departments and agencies use commercial off-the-shelf (COTS) security products and services to track, detect, or counter known vulnerabilities. A problem with many of these products is that different products use different names for the same vulnerabilities. Without a consistent vulnerability terminology, it is hard to compare the vulnerability coverage of such security products. Also, it may be difficult to correlate alerts among different vendors' or services' databases and tools.

CVE compatible products and services, however, use the same name for each vulnerability thus addressing many of these coverage and correlation concerns. Therefore, it is important that we consider acquiring CVE compatible security products and services. We should be careful, however, to consider CVE compatibility only for products and services that inherently make use of vulnerability names. Such products and services include vulnerability scanners, vulnerability databases, vulnerability advisory services, vulnerability patch services, most intrusion detection systems, and some firewalls.

Your organization's use of CVE-compatible products can assist you by

1) determining which product covers the vulnerabilities most applicable to an agency's network infrastructure; and

2) increasing the assurance that the alerts produced by the product(s) you choose will be able to be correlated with alerts from your other products and from your incident response center.

The requirements for CVE compatibility are described at http://cve.mitre.org/compatible/requirements.html. Currently identified compatible products and services are listed on the Compatible Products pages, http://cve.mitre.org/compatible. While CVE compatibility should be an important consideration in IT security product and service acquisition, federal departments and agencies should foremost consider their overall requirements (functionality, cost, performance, architecture, etc.) when acquiring products and services.

2. Federal departments and agencies should periodically monitor their systems for applicable vulnerabilities listed in the CVE vulnerability naming scheme.

We recommend monitoring systems for vulnerabilities included in the CVE list since it is a standardized, reviewed, and comprehensive vulnerability repository. CVE consists of both standardized and candidate vulnerabilities, and systems should be monitored for both types. Agencies should identify the CVE entries that apply to the software used in their systems and correct those vulnerabilities. Greater emphasis should be placed upon systems that are accessible from the Internet (e.g., web servers), systems that house important or sensitive applications or data (e.g. databases), or network infrastructure components (e.g. routers, switches, and firewalls). Since it is infeasible for an organization to find and fix all vulnerabilities in every system

simultaneously, organizations should carefully prioritize their monitoring and patching efforts in order to correct the most severe vulnerabilities on the most high-risk systems.

Automated software tools can scan hosts and networks for CVE vulnerabilities and we recommend regular use of such products. However, such products may not check for every CVE vulnerability entry. For additional thoroughness, systems administrators and security officers can periodically compare the software products used on systems directly to the entries listed in the CVE repository. Several commercial services exist that offer this type of functionality, but some do not contain all CVE vulnerabilities. In order to ensure complete CVE coverage, we recommend performing this comparison using the NIST ICAT Metabase (http://icat.nist.gov). ICAT is a publicly available CVE search engine that allows one to search for vulnerabilities by vendor names, products names, and version numbers. When an applicable vulnerability is found, ICAT provides a variety of vulnerability attributes (e.g. attack range and damage potential) and links to vulnerability and patch information from a variety of public resources. In summary, we recommend the use of automated scanning tools on a frequent basis combined with periodic manual vulnerability discovery using ICAT.

3. Federal departments and agencies should use the CVE vulnerability naming scheme in their descriptions and communications of vulnerabilities

Agencies should use CVE in their internal reports of vulnerability scans, notifications to system owners of observed vulnerabilities, and alerts identifying the vulnerabilities targeted by active exploits. Use of CVE will help to minimize confusion regarding which vulnerability is being referenced and provides an excellent check on whether the referenced vulnerability has been eliminated.

Agencies should also use CVE in communicating information about vulnerabilities externally. For example, communications to FedCIRC or other incident response teams should reference, where known, the CVE vulnerability name that newly observed exploits are targeting. Also, communications with vendors will be more accurate if CVE numbers are used. If 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. Also, communications with vendors of scanning tools regarding false positives or false negatives will be clearer if the offending vulnerability is labeled by CVE number.