ITL BULLETIN FOR DECEMBER 2013

THE NATIONAL VULNERABILITY DATABASE (NVD): OVERVIEW

Harold Booth, Doug Rike and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

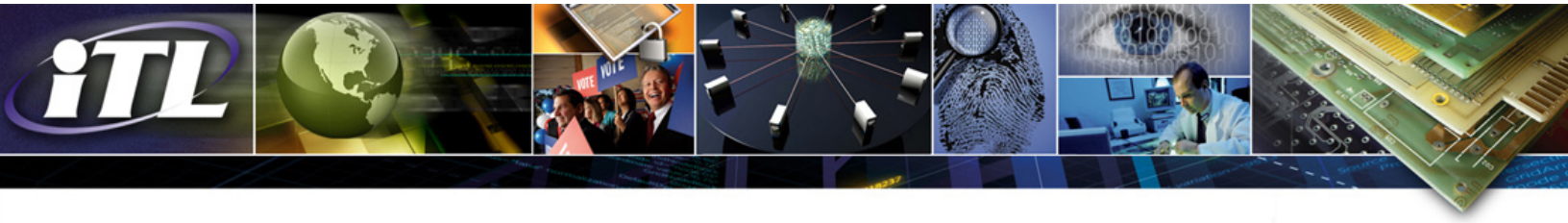
The National Vulnerability Database (NVD) and its companion, the National Checklist Program (NCP) repository, provide a valuable and flexible set of services to users around the world. The NVD was established in 2005 to provide a U.S. government repository of data about software vulnerabilities and configuration settings, while leveraging open standards to provide reliable and interoperable information about vulnerability impact metrics, technical assessment methods, IT product identification data, and references to remediation assistance.

The NVD is a product of the NIST Information Technology Laboratory's (ITL) Computer Security Division (CSD) and is sponsored by the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US-CERT) to provide timely vulnerability management information. The NVD provides a searchable interface and data feeds to help inform the public about the nature and severity of the hundreds of new vulnerabilities and variants discovered every month. IT administrators can use the NVD to prioritize the vulnerabilities to address in order to protect important systems. The NVD data feed information is used by both public and private sector consumers. For example, US-CERT's weekly bulletins are generated directly from the NVD data feeds; Payment Card Industry Security Standards Council Data Security Standards (PCI SSC DSS) compliant systems must remediate vulnerabilities above a particular threshold; and some vulnerability management product vendors use NVD information as a starting reference source for their scanners and feeds.

Vulnerability Analysis

NIST provides ongoing analysis of Common Vulnerabilities and Exposures (CVEs) and assigns Common Vulnerability Scoring System (CVSS) base metrics for each vulnerability, and will update a score if more information becomes available. Ongoing analysis and scoring helps NVD users to understand the potential severity of each issue, and helps users to prioritize vulnerability management activities. NIST works directly with vendors and researchers to improve the quality of the published data and to provide the public with accurate scoring data.

NIST partners with other national organizations to extend the international reach of the NVD. Organizations such as the Japan Vulnerability Network (JVN) and Spain's National Institute of Communications Technologies (INTECO) cooperate regarding the data that is analyzed and published by NIST through the NVD. International cooperation enables global consumers to continually monitor security posture, prioritize risk management, and coordinate effective response using a shared understanding of the possible vulnerabilities.



Use of Open Data Exchange Formats

To improve data interoperability, the NVD publishes data based upon the specifications in the Security Content Automation Protocol (SCAP) described in NIST Special Publication 800-126 Revision 2. SCAP is a multipurpose protocol that provides an automated means to collect and assess the state of devices. SCAP supports automated vulnerability checking, patch installation verification, security configuration checking, and assessment for indicators of compromise. SCAP content can be used by any tool that is conformant to the specifications.

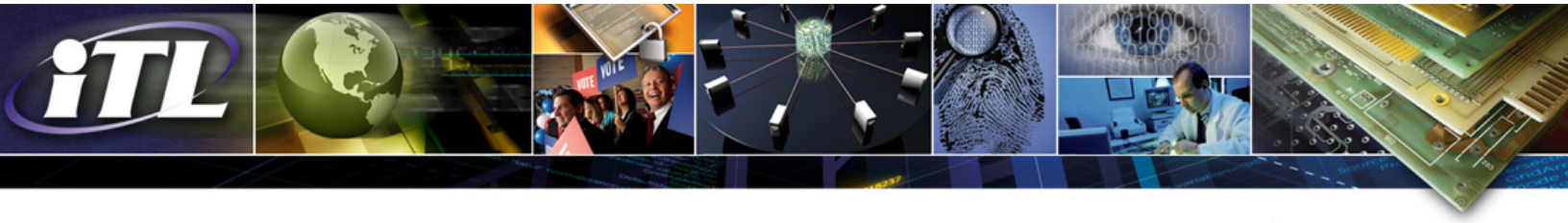
The following selected SCAP specifications and complementary models support the work of the NVD and NCP:

- Common Vulnerabilities and Exposures (CVE) - a common identifier assigned to a vulnerability to facilitate the sharing of relevant information about that flaw;
- Common Vulnerability Scoring System (CVSS) – a set of metrics for communicating the characteristics and impacts of IT vulnerabilities. NVD analysts provide a baseline analysis of the potential severity of a given vulnerability, based on publicly available information from researchers and vendors;
- Common Platform Enumeration (CPE) – a software enumeration that assists in communicating the hardware and software platforms that may be affected by a given vulnerability. Use of CPE enables users (and automated tools) to quickly identify vulnerabilities that may affect systems under their purview;
- Common Configuration Enumeration (CCE) – a set of unique platform-based identifiers associated with security configuration statements. CCE supports evaluation of configuration compliance with a given security configuration baseline; and
- Common Weakness Enumeration (CWE) – a taxonomy for identifying the common sources of software flaws (e.g., buffer overflows, failure to check input data). Where practical, NVD associates a given CVE vulnerability to the underlying CWE weakness.

National Checklist Program (NCP)

In addition to the NVD, NIST maintains the National Checklist Program Repository, a publicly available repository that contains information on a variety of security configuration checklists for specific IT products or categories of IT products. The site is an important component of the National Checklist Program (NCP) that was established to facilitate development of security configuration checklists and to meet the requirements of the Cyber Security Research and Development Act of 2002. By providing a central location for well-written, standardized checklists, NCP supports increased quality, usability, and availability of documents such as security configuration checklists, hardening guides, and benchmark configurations. Such checklists can reduce the vulnerability exposure of IT products and be particularly helpful to small organizations and individuals in securing their systems.

The NCP is described in detail in NIST Special Publication 800-70 Revision 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*. This publication describes the process for submitting and maintaining checklists, and it points out that "checklists can be developed, not only by IT vendors, but also by other organizations with technical competence in IT product security. A security configuration checklist might include any of the following:



- Configuration files that automatically set or verify various security settings;
- Documentation that guides the checklist user to manually configure an IT product;
- Documents that explain recommendations to securely install/configure a device; and,
- Policy documents that set forth security guidelines."

SP 800-70 describes NIST's tiers of checklists. Tier I checklists are prose-based, Tier II checklists document their recommended security settings in a machine-readable but nonstandard format, and Tier III checklists use SCAP to document their recommended security settings in machine-readable standardized SCAP formats. Tier IV checklists are SCAP files that have been validated to ensure interoperability with SCAP-validated products. Section 5 of SP 800-70 describes the methods for testing checklists to be submitted and for submitting them for NCP inclusion. For additional information about SCAP, including content validation tools (e.g., the SCAP Content Validation Utility, *SCAPVAL)*, please visit this website.

The NVD's web services and associated data models help risk managers protect proprietary information and avoid potential disclosure of critically sensitive data by providing the following resources (as of October 2013):

- Over 58,000 vulnerability advisories, of which almost three quarters have been translated into Spanish;
- 52 SCAP-expressed checklists that can be used by SCAP-validated security products to perform automated evaluations of system state;
- 173 non-SCAP checklists (e.g., English prose guidance and configuration scripts);
- 248 US-CERT alerts and 2,771 US-CERT vulnerability summaries; and
- Platform/product dictionary with over 79,000 operating system, application, and hardware name entries.

E-mail Announcements and Communications

The Vulnerability Management and SCAP communities are public/private partnerships consisting of interested parties from industry, research and educational institutions, and government working to advance automation and standardization of technical security operations. NIST participates in numerous discussion groups including the NVD Announcements List, the Checklist/SCAP Announcements List, the SCAP Discussion List, the XCCDF Discussion List, and the Emerging Specifications Discussion List. Information on joining these discussions, or obtaining automated NVD data, is available at the NVD website.

Information about NIST's information security programs, standards, guidelines, and related publications is available from the Computer Security Resource Center.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov