Two new SCAP documents help improve automating computer security management

March 16 2011

It's increasingly difficult to keep up with all the vulnerabilities present in today's highly complex operating systems and applications. Attackers constantly search for and exploit these vulnerabilities to commit identity fraud, intellectual property theft and other attacks. The National Institute of Standards and Technology has released two updated publications that help organizations to find and manage vulnerabilities more effectively, by standardizing the way vulnerabilities are identified, prioritized and reported.

Computer security departments work behind the scenes at government agencies and other organizations to keep computers and networks secure. A valuable tool for them is security automation software that uses NIST's Security Content Automation Protocol (SCAP). Software based on SCAP can be used to automatically check individual computers to see if they have any known vulnerabilities and if they have the appropriate security configuration settings and patches in place. Security problems can be identified quickly and accurately, allowing them to be resolved before hackers can exploit them.

The first publication, The Technical Specifications for the Security Content Automation Protocol (SCAP) Version 1.1 (NIST Special Publication (SP) 800-126 Revision 1) refines the protocol's requirements from the SCAP 1.0 version. SCAP itself is a suite of specifications for standardizing the format and nomenclature by which security software communicates to assess software flaws, security configurations and software inventories.

SP 800-126 Rev. 1 tightens the requirements of the individual specifications in the suite to support SCAP's functionality and ensure interoperability between SCAP tools. It also adds a new specification—the Open Checklist Interactive Language (OCIL)—that allows security experts to gather information that is not accessible by automated means. For example, OCIL could be used to ask users about their recent security awareness training or to prompt a system administrator to review security settings only available through a proprietary graphical user interface. Additionally, SCAP 1.1 calls for the use of the 5.8 version of the Open Vulnerability and Assessment Language (OVAL).

NIST and others provide publicly accessible repositories of security information and standard security configurations in SCAP formats, which can be downloaded and used by any tool that complies with the SCAP protocol. For example, the NIST-run National Vulnerability Database (NVD) provides a unique identifier for each reported software vulnerability, an analysis of its potential damage and a severity score. The NVD has grown from 6,000 listings in 2002 to about 46,000 in early 2011. It is updated daily.

The second document, Guide to Using Vulnerability Naming Schemes (Special Publication 800-51 Revision 1), provides recommendations for naming schemes used in SCAP. Before these schemes were standardized, different organizations referred to vulnerabilities in different ways, which created confusion. These naming schemes "enable better synthesis of information about software vulnerabilities and misconfigurations," explained co-author David Waltermire, which minimizes confusion and can lead to faster security fixes. The Common Vulnerabilities and Exposures (CVE) scheme identifies software flaws; the Common Configuration Enumeration (CCE) scheme classifies configuration issues.

SP 800-51 Rev.1 provides an introduction to both naming schemes and makes recommendations for using them. It also suggests how software and service vendors should use the vulnerability names and naming schemes in their products and service offerings.

More information: The Technical Specifications for the Security Content Automation Protocol (SCAP) Version 1.1 (NIST Special Publication 800-126 Revision 1) can be found at csrc.nist.gov/publications/nis … rev1/SP800-126r1.pdf . The Guide to Using Vulnerability Naming Schemes (Special Publication 800-51 Revision 1) can be found at csrc.nist.gov/publications/nis … ev1/SP800-51rev1.pdf .

Provided by National Institute of Standards and Technology