

June 2006 (vol. 7, no. 6), art. no. 0606-o6004  
1541-4922 © 2006  
Published by the IEEE Computer Society

## News

# Functionality Meets Terminology to Address Network Security Vulnerabilities

Greg Goth

**I**n 1999, when most of the computer industry's cautionary buzz centered on finding and fixing Y2K flaws, a small group of MITRE engineers began work on the [Common Vulnerabilities and Exposures dictionary](#). Prior to CVE, no standard nomenclature existed for network security holes. In fact, the security landscape was rife with different names for the same vulnerability, as vendors strove to differentiate themselves from competitors. As a result, network administrators often found themselves performing redundant searches for the same shortcoming, wasting time and effort.

Security vendors and administrators welcomed the CVE effort almost from the start, but the supporting infrastructure around it, enabling a wider variety of end users to deploy CVE-compatible technology, has taken time to dovetail with the dictionary. Not until August 2005 did the National Institute of Standards and Technology (NIST) launch its [National Vulnerability Database](#), which is updated with CVE data in real time. The NVD also includes data-analysis and fine-grained search capabilities.

"With 300-plus products and services using the CVE name, we definitely need a database of information relative to the CVE standard, and the NVD database provides that," says Peter Mell, senior computer scientist at NIST and NVD project leader. "End users need a way to prioritize the constant stream of vulnerabilities that are coming out—it's up to about 17 a day. The IT organizations need to answer the questions of 'Do I panic right now?' or 'Can this be part of my usual configuration management update I do in two weeks?' By integrating the NVD and CVE, we've made a significant step toward helping people to do that."

## What's in a name?

The NVD currently gets almost 2 million hits each month, of which Mell estimates 1.6 million are downloads of real value. "That's much more than I had suspected," he says, "so it's really being actively used. But, ultimately, when you think of the active worldwide security community, a lot more people could know about it and use it."

Gary Miliefsky, founder and CTO of NetClarity, a network security vendor that features CVE-

compatible tools, has been a longtime CVE champion. He says that even within the past few months, he's met blank stares at conferences when he mentions CVE.

"If we had a term that was plain English that scared the bejesus out of people, that would be good," Miliefsky says. "If somebody tells you you have a worm infecting your machine, you get concerned. But if somebody tells you you have a buffer overflow on port x, it doesn't tend to alarm the typical person."

As an example of Miliefsky's point, the name "Nimda" might concisely bring back memories of the network-clogging worm that spread in September 2001. But "CVE-2001-0333" and its associated description, "Directory traversal vulnerability in IIS 5.0 and earlier allows remote attackers to execute arbitrary commands by encoding .. (dot dot) and '\ ' characters twice //" doesn't strike fear in the hearts of the typical user—even though the worm couldn't affect systems that repaired the hole.

"There's got to be a way, in plain English, to make people aware of the root cause—the root cause—of downtime and out-of-compliance issues when it comes to network security; and people don't know it's not the virus or worm, it's the hole that's being exploited. And they don't know that, and it has to get out there somehow."

Particularly frustrating to Miliefsky and other CVE proponents is the "almost there" status of so much of both the technical and procedural infrastructure supporting ubiquitous deployment:

- The engineers behind the CVE and NVD initiative have also created the Open Vulnerability Assessment Language. OVAL standardizes vulnerability queries in a three-step XML-based process that eliminates the time-consuming and mistake-laden need for network administrators to interpret a panoply of text-based information from various vendors, public agencies, and consultants.
- Legislative and regulatory bodies have adopted stringent reporting standards around laws such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Standardizing network auditing around CVE standards represents a next step toward accepting universal nomenclature of network weaknesses.
- The international community has taken to the CVE nomenclature, which is decided upon by an editorial board of industry, research, and academic experts. Bob Martin, MITRE's CVE Compatibility Lead, says more than 300 products and services from 23 nations are CVE-compatible.
- CVE-compatible products have shown themselves to be cost-effective. Larry Pesce, manager of information systems security for Care New England, a Rhode Island-based healthcare network, says the use of a CVE-compatible penetration testing tool by vendor Core Security probably saves the organization the cost of one to two full-time employees

a year. Billy Austin, chief security officer of Saint, a CVE-compatible vendor, says using such tools saves the typical security administrator 2.5 hours per vulnerability over doing manual searches.

### **Unrevolutionary progress**

Yet, even CVE proponents concur that industry hasn't picked up on the concept as quickly as it might. The reasons are numerous.

"What we've done to date has been very successful, and I think we've done a good job," Mell says. "Certainly, there's room for improvement, and we're taking steps to do that, but—and it's a big but—what we're doing is helpful but not revolutionary, in terms of how the industry does things." This leaves the door wide open for people to propose new ideas that will purportedly solve everything perfectly. Regulators and lawmakers join companies and industry organizations who are trying to address the problem from their different points of view. "And the trouble," Mell concludes, "is many of those have gone astray of the goal they really wanted, which was to secure the system."

Mell sees more completely automated auditing and configuration capabilities as the possible linchpin to ubiquitous deployment of CVE-compatible technology. XML Configuration Checklist Data Format is a specification language developed by the National Security Agency and NIST. Using it together with CVE and OVAL will let network administrators satisfy regulatory network security requirements dynamically and reconfigure their networks at the same time.

"We realized these security checklists are static information on securing an application," he says, "and you could couple that with dynamic information about every known vulnerability about that product. So, you could link the NVD and the checklist together and get both sets of information."

Successfully combining these dynamic network assurance technologies would be boons for network administrators striving to meet due diligence requirements under regulations such as HIPAA, Mell says. MITRE's Martin says the XML-based OVAL technology is "an auditor's dream," because it will standardize vulnerability and flaw information currently written in text, rife with inconsistencies, and often leading to redundant evaluation for what might be the same flaw. In fact, the US Defense Department has already mandated that its vulnerability technology vendors supply CVE- and OVAL-compatible tools. Widespread adoption of these technologies, Martin wrote in an article appearing in *Crosstalk: The Journal of Defense Engineering*, will enable the DoD to transform its Information Assurance Vulnerability Alert process to predominantly machine-to-machine information flows. Automating the IAVA process, Martin says, "will improve the accuracy, timeliness, and manpower needed to address the flaws that are found in software."

Mell says vendors must now increase their efforts to broaden the OVAL technology to bring those increased capabilities to fruition.

"The big hurdle, and this has always been a hurdle, is trying to get enough OVAL queries," he says. "MITRE has funding to create OVAL queries, but there are just too many vulnerabilities for a single entity with a modest amount of funding to generate the necessary number." Mell thinks that getting vendors involved in writing OVAL queries is the next step in moving CVE significantly forward.

### **New efforts round out the landscape**

While the community around CVE and OVAL continues its work, MITRE researchers have recently introduced two new technologies intended to work hand in glove with them:

- **Common Weakness Enumeration.** CWE includes not only CVE information but also community-commissioned information intended to serve as a standard taxonomic base for measuring common classes of flaws and their mitigation tools.
- **Common Malware Enumeration.** CME is still in its initial operational phase. It's intended to standardize virus nomenclature. As with pre-CVE vulnerabilities, different vendors often call the same virus by different names.

Martin describes CWE as "an encyclopedia that describes all the things we are trying to avoid in code design and architecture that lead to exploitable vulnerabilities. The premise is to bring the industry together around an agreed-upon terminology, an agreed-upon description of flaws and how they work, and the inherent risk from them." This will give developers more flexibility to decide which technologies to use.


**W**hen and if all these elements come together, Martin sees a day where network administrators will have much greater influence over the design and deployment of security architectures. Increased use of these standards will free these executives to compel their vendors to adhere to standards instead of feeling locked in to a vendor's technology.

"That's a different way of thinking," he says. "People are so used to selecting the vendor and that's kind of the core they build out from. What we want them to do is get married to enabling standards and then build around that."

### **Related Links**

---

 [DS Online's Security Community](#)

 ["Integrated Vulnerability Management System for Enterprise Networks," Proceedings of EEE 05](#)



"Can Source Code Auditing Software Identify Common Vulnerabilities and Be Used to Evaluate Software Security?" Proceedings of HICSS 04

---

**Cite this article:**

Greg Goth, "Functionality Meets Terminology to Address Network Security Vulnerabilities," *IEEE Distributed Systems Online*, vol. 7, no. 6, 2006, art. no. 0606-o6004.