

2004 News — Archive

December 22, 2004

Gentoo Foundation Makes CVE Compatibility Declaration

Gentoo Foundation has declared that its Gentoo Linux Security Advisories will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services](#) page.

KDware Ltd. Makes CVE Compatibility Declaration

KDware Ltd., has declared that its incident management tool, Incident MiND, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services](#) page.

CVE Mentioned in Article about Developers Preventing Security Problems in eWeek

CVE was mentioned in a December 2004 article in eWeek Magazine entitled "An Applications View on Security." The main topic of the article is a discussion about developers preventing security problems and that "three application firewall vendors—Teros Inc., NetContinuum Inc. and Imperva Inc.—threw down a challenge to other security vendors to submit their products to independent testing by International Computer Security Association Labs (a division of TruSecure Corp.) to determine their effectiveness against application-level attacks."

CVE was mentioned in a quote by Gary Miliefsky, CEO of PredatorWatch Inc., who states: "Most developers don't make adequate use of the Common Vulnerabilities and Exposures data at [cve.mitre.org](#). I was speaking to a group the other night, and I said, 'Raise your hand if you know what a CVE is.' No one raised their hand. A developer needs to know when a product is opening a port or using any other resource what vulnerabilities it's opening."

PredatorWatch, Inc. is listed on the [CVE-Compatible Products and Services](#) page and its PredatorWatch Auditor 128 and Update Service, PredatorWatch Auditor 16 and Update Service, and PredatorWatch Auditor Enterprise and Update Service each recently received official "Certificates of CVE Compatibility" at MITRE's compatibility awards ceremony on November 18, 2004 at the CSI Computer Security Conference in Washington, D.C., USA.

CVE Mentioned in Article about OVAL in Information Security Magazine

CVE was mentioned in an article entitled "'Big O' For Testing" in the December 2004 issue of Information Security Magazine. In the article the author describes MITRE Corporation's OVAL project and states: "The Open Vulnerability Assessment Language (OVAL) project, headed by nonprofit MITRE and funded by the Department of Homeland Security's U.S.-CERT, is being developed as a standardized process by which security tool creators, operating system vendors and security professionals test systems for exploitable vulnerabilities. XML-based OVAL leverages MITRE's Common Vulnerabilities and Exposures (CVE) Initiative . . . [and] gives security managers the ability to test for a particular CVE vulnerability in OVAL-compliant applications and platforms. OVAL will tell testers whether vulnerable software is installed and, if so, whether it has a vulnerable configuration."

MITRE's OVAL Web site is listed on the [CVE-Compatible Products and Services](#) page and OVAL-IDs are included as references in CVE names when applicable.

CVE Mentioned in Product Review Article in Network Computing

CVE was mentioned briefly in a December 7, 2004 product test article in Network Computing's Security Pipeline entitled "Test Run: PredatorWatch's Auditor 128." CVE was mentioned in the second paragraph of the review, in which the author states: "To identify vulnerabilities and test compliance to HIPAA, Sarbanes-Oxley, ISO-17799 and other regulations, [PredatorWatch] Auditor uses the CVE (Common Vulnerabilities and Exposures) dictionary of known threats."

PredatorWatch, Inc. and PredatorWatch Auditor 128 and Update Service are listed on the [CVE-Compatible Products and Services](#) page, along with its PredatorWatch Auditor 16 and Update Service and PredatorWatch Auditor Enterprise and Update Service. All three of these products are listed as officially CVE-Compatible.

December 8, 2004

netVigilance, Inc. Makes CVE Compatibility Declaration

netVigilance, Inc. has declared that its network scanning appliance, EagleBox, is CVE-compatible. In addition, netVigilance, Inc.'s SecureScout NX, SecureScout SP, and SecureScout Perimeter are also listed on the [CVE-Compatible Products and Services](#) page. For additional information about these and other CVE-compatible products, visit the [CVE-Compatible Products and Services](#) page.

Privacyware Makes CVE Compatibility Declaration

Privacyware has declared that its host-based intrusion prevention product for Microsoft Web Servers, ThreatSentry, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services](#) page.

ReddShell Corporation Makes CVE Compatibility Declaration

ReddShell Corporation has declared that its vulnerability assessment and management tool, SECUREScan, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services](#) page.

Xacta Corporation Makes CVE Compatibility Declaration

Xacta Corporation has declared that its risk management capability, Xacta IA Manager, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services](#) page.

"Certificate of CVE Compatibility" Awarded to Trend Micro, Inc.

Trend Micro, Inc. was recently presented with a "Certificate of CVE Compatibility" for its Trend Micro Vulnerability Assessment product. MITRE held an awards ceremony at CSI's Computer Security Conference in Washington, D.C., USA on November 18th to award compatibility certificates to 10 organizations for 20 information security products or services. Trend Micro received its certificate in a special ceremony on December 2nd at MITRE in Bedford, Massachusetts.

TrendMicro - CVE Compatible

Robert A. Martin, CVE Compatibility Lead, and John Hermano, Vulnerability Assessment Product Manager, Trend Micro, Inc., in a special ceremony at MITRE.

Trend Micro, Inc. and its Trend Micro Vulnerability Assessment product are listed on the CVE-Compatible Products and Services page.

Seven "Certificates of CVE Compatibility" Awarded to Internet Security Services, Inc.

Internet Security Services, Inc. (ISS) was awarded "Certificates of CVE Compatibility" for 7 products at an awards ceremony at CSI's Computer Security Conference in Washington, D.C., USA on November 18, 2004. The products receiving compatibility certificates included X-Force Database, X-Force Alerts and Advisories, Internet Scanner, System Scanner, RealSecure Network 10/100 and Network Gigabit, RealSecure Server Sensor, and SiteProtector. ISS was one of 10 of the most recent organizations to achieve the final phase of MITRE's formal CVE Compatibility Process and to have their information security products and services registered as officially "CVE-compatible." The awards, 20 in all, were presented at the ceremony by Lawrence C. Hale, Deputy Director of the National Cyber Security Division, U.S. Computer Emergency Readiness Team (US-CERT) at the U.S. Department of Homeland Security.

CSI '04

Lawrence C. Hale, US-CERT/DHS and Peter Allor, Director of X-Force Intelligence, Internet Security Systems, Inc. (ISS) and Lori Bauer of ISS, at MITRE's compatibility awards ceremony at CSI Computer Conference.

Internet Security Services, Inc. and its X-Force Database, X-Force Alerts and Advisories, Internet Scanner, System Scanner, RealSecure Network 10/100 and Network Gigabit, RealSecure Server Sensor, and SiteProtector are listed on the CVE-Compatible Products and Services page.

Two "Certificates of CVE Compatibility" Awarded to Symantec Corporation

Symantec Corporation was awarded "Certificates of CVE Compatibility" for its DeepSight Alert Services and its SecurityFocus Vulnerability Database at an awards ceremony at CSI's Computer Security Conference in Washington, D.C., USA on November 18, 2004. Symantec was one of 10 of the most recent organizations to achieve the final phase of MITRE's formal CVE Compatibility Process and to have their information security products and services registered as officially "CVE-compatible." The awards, 20 in all, were presented at the ceremony by Lawrence C. Hale, Deputy Director of the National Cyber Security Division, U.S. Computer Emergency Readiness Team (US-CERT) at the U.S. Department of Homeland Security.

CSI '04

Lawrence C. Hale, US-CERT/DHS, and Dee Liebenstein, Group Product Manager for DeepSight Threat Management Services at Symantec Corporation, at MITRE's compatibility awards ceremony at CSI Computer Conference.

Symantec Corporation and its DeepSight Alert Services and SecurityFocus Vulnerability Database are listed on the CVE-Compatible Products and Services page.

CVE Included in Article Advocating Proactive Network Security on ZDNet

CVE was mentioned throughout a November 30, 2004 article on ZDNet entitled "A guide to proactive network security." In the article the author uses CVE names as a synonym for computer vulnerabilities: ". . . a single enterprise can spend thousands on firewalls, VPNs, antivirus and IDS systems, while the real network security culprits, "Common Vulnerabilities and Exposures" (CVEs), go largely undetected. CVEs are essentially holes in applications that can be attacked by hackers and cyber terrorists to steal information or bring down networks. CVEs are a real problem and according to the 2004 E-Crime Survey are the systemic cause of over 90 percent of all network security breaches."

The author advocates a number of steps to proactive network security including developing and employing a security policy, locking down mobile devices, turning on wireless encryption, using and patching routers, using firewalls, downloading and installing commercial-grade security tools, disabling potentially exploitable browser objects, constantly keeping up with the latest threats, and closing known vulnerabilities. The author states: "But preventing the attack with a vulnerability management system to eliminate CVEs is the most important component [of proactive network security]."

Regarding closing known vulnerabilities the author states: "Known weaknesses in systems are called Common Vulnerabilities and Exposures (CVEs), compiled and documented by the MITRE organization. These vulnerabilities should be eliminated from every system on your network by applying patches or taking other actions, as required. Technology is available to automatically detect and eliminate CVEs. More information is detailed at the cve.mitre.org Web site."

CVE Mentioned in PredatorWatch, Inc. Press Release

CVE was mentioned in a November 5, 2004 press release by PredatorWatch, Inc. about its Auditor 128 product entitled "PredatorWatch Launches World's Most Comprehensive Enterprise Security Management Appliance for Small- to Mid-Sized Networks." CVE is mentioned in the second paragraph of the release, which states: "A single business can spend hundreds or even thousands of dollars on countermeasures such as intrusion detection systems, firewalls and anti-virus software, while the real network security culprits are common vulnerabilities and exposures (CVEs). CVEs, anything that can be exploited on any computer, are the systemic cause of over 95% of all network security breaches."

CVE is also mentioned in a quote by a PredatorWatch customer, Stephen Irish, executive vice president, Enterprise Bank and Trust Company, who states: ". . . the company's technology helps ensure newly deployed servers are locked down and allows us to remain up-to-date on the latest vulnerabilities and exposures on the CVE List. The technology also detects and diagnoses potential security flaws that could cause our bank to be at risk and non-compliant with GLBA and FDIC requirements."

PredatorWatch, Inc. is listed on the CVE-Compatible Products and Services page and its PredatorWatch Auditor 128 and Update Service, PredatorWatch Auditor 16 and Update Service, and PredatorWatch Auditor Enterprise and Update Service each recently received official "Certificates of CVE Compatibility" at MITRE's compatibility awards ceremony on November 18th at the CSI Computer Security Conference in Washington, D.C., USA.

November 23, 2004

MITRE Presents CVE Compatibility Certificates in Awards Ceremony at CSI Computer Security Conference

MITRE held an awards ceremony on Monday evening, November 18th at Computer Security Institute's (CSI) 31st Annual Computer Security Conference and Exhibition in Washington, D.C., USA, to present "Certificates of CVE Compatibility" to the 10 most recent organizations to achieve the final phase of MITRE's formal CVE Compatibility Process and whose 20 information security products or services are now officially

"CVE-compatible." The awards were presented by Lawrence C. Hale, Deputy Director of the National Cyber Security Division, U.S. Computer Emergency Readiness Team (US-CERT) at the U.S. Department of Homeland Security.

Organizations participating in the ceremony included Citadel Security Software Inc.; eEye Digital Security; Internet Security Systems, Inc.; nCircle Network Security, Inc.; PredatorWatch, Inc.; SAINT Corporation; and Symantec Corporation. Organizations receiving certificates but unable to participate in the ceremony were DragonSoft Security Associates, Inc.; Trend Micro, Inc.; and Venus Information Technology, Inc.

CSI '04

MITRE's CVE Compatibility awards ceremony at the CSI Computer Conference. Front row left to right, Gary Miliefsky, PredatorWatch, Inc.; Doug Eames, PredatorWatch, Inc.; and Kent Landfield, Citadel Security Software Inc. Back row left to right, Pete Tasker, MITRE Corporation; Peter Allor, Internet Security Systems, Inc.; Lori Bauer, Internet Security Systems, Inc.; Lawrence C. Hale, US-CERT/DHS; Gene Skiba, eEye Digital Security, Inc.; Mike Murray, nCircle Network Security, Inc.; Dee Liebenstein, Symantec Corporation; and Sam Kline, SAINT Corporation.

For additional information about CVE compatibility and to review all products and services listed, visit the [CVE Compatibility Process](#) and [CVE-Compatible Products and Services](#) pages.

Citadel Security Software Inc. Issues Press Release Announcing Receipt of "Certificate of Compatibility for Full CVE Compliance"

CVE compatibility was the main topic of a November 9, 2004 press release by Citadel Security Software Inc. entitled "Citadel Security Software's Hercules Awarded Certificate of Compatibility for Full CVE Compliance." In the release Citadel announces that its ". . . [Automated Vulnerability Remediation] solution, Hercules, has been certified as fully compliant and compatible with the Common Vulnerabilities and Exposures (CVE) Initiative."

The release included a quote by Carl Banzhof, CTO of Citadel Security Software, who states: "Prior to this award ceremony, only 14 products or services from 10 organizations had achieved the final phase of MITRE's formal CVE Compatibility Process and become officially CVE-compatible. We are proud to be the first automated vulnerability remediation solution to meet the CVE compatibility requirements. By achieving full CVE compatibility for Hercules, our customers now have better vulnerability coverage, easier interoperability and enhanced security across the enterprise." The release also included a quote by Kent Landfield, a CVE Editorial Board member since 1999 and Security Group Director for Citadel, who states: "The CVE Initiative brings consistency and interoperability to the security and computing community. The CVE Compatibility Process is a formal evaluation of submitted information security products and services. The testing and certification process assures products meet the criteria set out by the CVE Initiative to prove they are CVE-compatible."

CSI '04

Lawrence C. Hale, US-CERT/DHS, and Kent Landfield, Security Group Director at Citadel Security Software Inc., at MITRE's compatibility awards ceremony at CSI Computer Conference.

Citadel Security Software Inc. and Hercules are listed on the [CVE-Compatible Products and Services](#) page.

DragonSoft Security Associates, Inc. Issues Press Release Announcing Recognition for CVE Compatibility

CVE compatibility was the main topic of a November 9, 2004 press release by DragonSoft Security Associates, Inc. entitled "ASIA Vulnerability Assessment Leader DragonSoft Awarded CVE-Compatibility Certificate." In the release DragonSoft announces that "DragonSoft is the first and only Taiwan security developer [to receive a Certificate of Official CVE Compatibility] among 125 security vendors in the world" and that receipt of the certificate is a major milestone for DragonSoft.

DragonSoft Security Associates, Inc. and DragonSoft Secure Scanner are listed on the [CVE-Compatible Products and Services](#) page.

eEye Digital Security Issues Press Release Announcing Receipt of Certificate of CVE Compatibility

CVE compatibility was the main topic of a November 9, 2004 press release by eEye Digital Security entitled "Vulnerability Management Leader eEye Digital Security Awarded CVE-Compatibility by MITRE Corporation." In the release eEye announces that "its industry-leading network security scanner Retina has been awarded compatibility with the Common Vulnerabilities and Exposures (CVE) . . ." The release also includes a quote by Firas Raouf, eEye's Chief Operating Officer, who states: "Retina's recognition as one of the first network security scanners to achieve CVE-compatibility demonstrates eEye's commitment to interoperability throughout the security industry. Our world-class research team has discovered more critical security vulnerabilities than any other, so we understand the compelling need for naming standards to effectively communicate these vulnerabilities to the security community."

CSI '04

Lawrence C. Hale, US-CERT/DHS, and Gene Skiba, Director of Federal Operations at eEye Digital Security, at MITRE's compatibility awards ceremony at CSI Computer Conference.

eEye Digital Security and Retina Network Security Scanner are listed on the [CVE-Compatible Products and Services](#) page.

nCircle Network Security, Inc. Issues Press Release Announcing Receipt of Certificate of CVE Compatibility

CVE compatibility was the main topic of a November 9, 2004 press release by nCircle Network Security, Inc. entitled "nCircle Recognized for Common Vulnerabilities Exposure Compatibility." In the release nCircle announces that it "has been formally recognized for Common Vulnerabilities Exposure (CVE) compatibility for its IP360 Vulnerability Management System." The release further states: "The award, presented to nCircle this week during the CSI Computer Security Conference in Washington, DC, recognizes security products that have incorporated MITRE Corporation's CVE names in its vulnerability search databases and other information security products and services."

The release also includes a quote by Tim Keanini, Chief Technical Officer at nCircle, who states: "nCircle actively supports standardization efforts in the security market, including the CVE's common lexicon for the vulnerability namespace. We are committed to ensuring nCircle's IP360 product continues to support CVE names, and provides customers with the best tools for vulnerability management."

CSI '04

Lawrence C. Hale, US-CERT/DHS, and Mike Murray, Director of Vulnerability and Exposure Research at nCircle Network Security, Inc. and Gene Skiba, Director of Federal Operations at eEye Digital Security, at MITRE's compatibility awards ceremony at CSI Computer Conference.

nCircle Network Security, Inc. and its IP360 Vulnerability Management System are listed on the [CVE-Compatible Products and Services](#) page.

SAINT Corporation Issues Press Release Announcing Receipt of "Certificate of CVE Compatibility" for SAINTbox and WebSAINT

CVE compatibility was the main topic of a November 9, 2004 press release by SAINT Corporation entitled "SAINTbox and WebSAINT Are Certified CVE-Compatible." In the release SAINT announces that "On Monday, November 8th, MITRE Corporation awarded their CVE (Common Vulnerabilities and Exposures) Certificate of Compatibility to two SAINT Corporation products: SAINTbox and WebSAINT. During an awards ceremony at the 31st Annual Computer Security Conference and Exhibition in Washington, D.C., SAINT Corporation was honored for their work in this effort and passing the final and most rigorous phase of the compatibility process. "

Also included in the release is a quote by Sam Kline, SAINT's Chief Development Engineer, who states: "We are pleased to be adding SAINTbox and WebSAINT to our growing suite of CVE-compatible tools. The CVE naming standard fills an important need in today's security community, and maintaining accurate references in all of our products has always been and will remain a high priority for us."

CSI '04

Lawrence C. Hale, US-CERT/DHS, and Sam Kline, Chief Engineer of SAINT Corporation, at MITRE's compatibility awards ceremony at CSI Computer Conference.

SAINT Corporation and its SAINTbox and WebSAINT products are listed on the CVE-Compatible Products and Services page.

DragonSoft Security Associates, Inc. Makes CVE Compatibility Declaration

DragonSoft Security Associates, Inc. has declared that its DragonSoft Vulnerability Database is CVE-compatible. In addition, DragonSoft's DragonSoft Secure Scanner is also listed on the CVE-Compatible Products and Services page. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Three Example Procurement Documents Added to CVE Web Site

Three example procurement documents have been added to the CVE Documents page to assist government agencies and other organizations with including CVE in the development of their request for proposals, statements of work, and other procurement requirements for the purchase of software applications as well for the acquisition of specific network and system assessment and remediation tools.

The following three example documents are available in Microsoft Word format:

- CVE-Relevant Software Supplier Requirements (SWSupplier) - This document is an extract of the statement of objectives used by the Department of Defense to explain the security-relevant requirements they wanted met by software suppliers. Several areas of security issues are addressed as well as the use of CVE names for vulnerabilities in security notifications.
- CVE-Relevant Vulnerability Assessment Tool Requirements (IAVMtool) - This document is an extract of the statement of work used by the Department of Defense to explain the security-relevant requirements they wanted met by an enterprise-wide vulnerability assessment and reporting tool. Several areas of security issues are addressed as well as the use of CVE names for vulnerabilities being reported.
- CVE-Relevant Remediation Tool Requirements (IAremedtool) - This document is an extract of the statement of work used by the Department of Defense to explain the security-relevant requirements they wanted met by an enterprise-wide remediation tool. Several areas of security issues are addressed as well as the use of CVE names for choosing which vulnerabilities are remediated and reporting remediation status.

Please contact us with any questions or for more information.

CVE Presents Briefing at New England Information Security Group Meeting

Robert A. Martin, CVE Compatibility Lead, presented a briefing about CVE and OVAL on November 18, 2004 entitled "Standards for Enabling Automation in Information Security" at the November Meeting of the New England Information Security Group in Boston, MA, USA. The presentation was successful and exposed CVE and OVAL to an audience of "individuals and organizations interested in securing their technical infrastructure." The group provides a venue to distribute information and educate the general membership on security products, techniques, and/or related issues.

Visit the CVE Calendar page for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

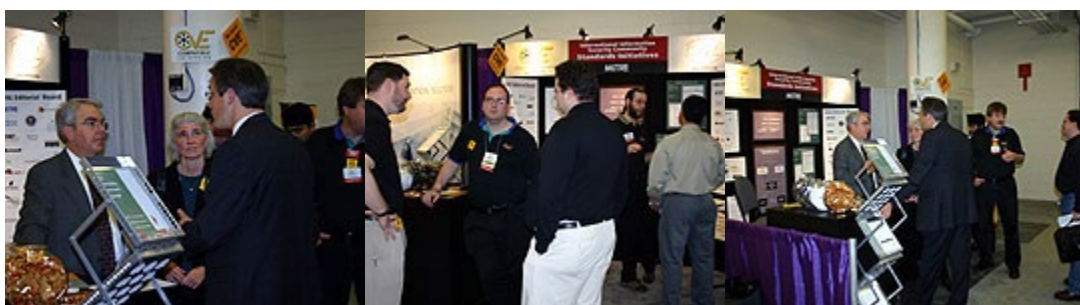
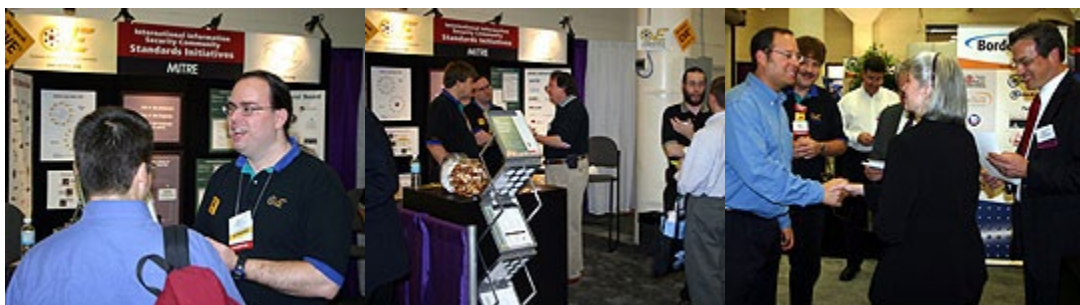
MITRE Hosts CVE/OVAL Booth at LISA 2004

MITRE hosted a CVE/OVAL exhibitor booth at LISA 2004, November 17-18, 2004, in Atlanta, Georgia, USA. The conference was successful and exposed CVE and OVAL to system and network administrators from industry, academia, and government.

Visit the CVE Calendar page for information about this and other upcoming events.

MITRE Hosts CVE/OVAL Booth at the CSI Computer Security Conference

MITRE hosted an CVE/OVAL exhibitor booth at the Computer Security Institute's (CSI) 31st Annual Computer Security Conference and Exhibition, November 8 - 10, 2004 in Washington, D.C., USA. The conference was successful and exposed CVE and OVAL to information security and network professionals from industry, academia, and government. See photos below:



Visit the CVE Calendar page for information about this and other upcoming events.

November 8, 2004

20 Additional Information Security Products/Services Now Registered as Officially "CVE-Compatible"

Twenty information security products and services from nine organizations are the latest to achieve the final stage of MITRE's formal CVE Compatibility Process and are now officially "CVE-compatible." Each product is now eligible to use the CVE-Compatible Product/Service logo, and

their completed and reviewed "CVE Compatibility Requirements Evaluation" questionnaires are posted as part of their product listings on the CVE-Compatible Products and Services page on the CVE Web site. Fourteen products from were previously declared officially compatible in February.

The following products are now registered as officially "CVE-Compatible":

- | | | |
|--------------------------------------|---|---|
| Citadel Security Software Inc. | - | Hercules |
| DragonSoft Security Associates, Inc. | - | Dragonsoft Secure Scanner |
| eEye Digital Security | - | Retina Network Security Scanner |
| Internet Security Systems, Inc. | - | X-Force Database
X-Force Alerts and Advisories
Internet Scanner
System Scanner
RealSecure Network 10/100 and Network Gigabit
RealSecure Server Sensor
SiteProtector |
| nCircle Network Security, Inc. | - | IP360 Vulnerability Management System |
| PredatorWatch, Inc. | - | PredatorWatch Auditor 16 and Update Service
PredatorWatch Auditor 128 and Update Service
PredatorWatch Auditor Enterprise and Update Service |
| SAINT Corporation | - | SAINTbox
WebSAINT |
| Trend Micro, Inc. | - | Trend Micro Vulnerability Assessment |
| Symantec Corporation | - | DeepSight Alert Services
SecurityFocus Vulnerability Database |
| Venus Information Technology, Inc. | - | Cybervision Intrusion Detection System |

Use of the official CVE-Compatible logo by these organizations will allow system administrators and other security professionals to look for the logo when adopting vulnerability management products and services for their enterprises. The compatibility process questionnaires will help end-users compare how different products satisfy the CVE compatibility requirements, and therefore which specific implementations are best for their networks and systems.

An awards ceremony was held tonight in the Vendor Track Presentation Theater at the Computer Security Institute's (CSI) 31st Annual Computer Security Conference and Exhibition, November 8, 2004, at the Marriott Wardman Park Hotel, in Washington, D.C., USA, to present Certificates of CVE Compatibility to the organizations that have achieved this final phase. Lawrence C. Hale, the Deputy Director of the National Cyber Security Division, U.S. Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security, presented the awards. Organizations participating in the ceremony included Citadel Security Software Inc.; eEye Digital Security; Internet Security Systems, Inc.; nCircle Network Security, Inc.; PredatorWatch, Inc.; SAINT Corporation; and Symantec Corporation.

For additional information about CVE compatibility and to review all products and services listed, visit the CVE Compatibility Process and CVE-Compatible Products and Services pages.

MITRE Hosts CVE/OVAL Booth at FIAC 2004

MITRE hosted a CVE/OVAL exhibitor booth at the Federal Information Assurance Conference (FIAC) 2004, October 26 - 27, 2004, at the University of Maryland University College in Adelphi, Maryland, USA. The conference was successful and exposed CVE and OVAL to network and systems administrators, security practitioners, acquisition and procurement officials, systems security officers, federal managers, accreditors, and certifiers from numerous agencies of the U.S. federal government.

Visit the CVE Calendar page for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

Conference Photos of CVE Booth at the SANS Network Security 2004

MITRE hosted an CVE/OVAL exhibitor booth at SANS Network Security 2004, September 30 - October 1, 2004 in Las Vegas, Nevada, USA. See photos below.



October 20, 2004

CVE Compatibility Milestone: 200 Products and Services Now Listed!

The CVE Initiative achieved a major milestone with 202 information security products and services now listed in the CVE-Compatible Products and Services section of the CVE Web site. These 200 products have been declared CVE-compatible or are in the process of being made compatible by 125 organizations from industry, government, and academia from around the world. Of these, 14 products/services from 10 organizations have achieved the final phase of MITRE's formal CVE Compatibility Process and are now officially CVE-compatible. These are indicated in the CVE-Compatible Products and Services section with the CVE-Compatible product/service logo.

"CVE-compatible" means that a product or service uses CVE names in a way that allows it to cross-link with other repositories that also use CVE names, as documented in the CVE compatibility requirements. Each item listed on the CVE Web site includes a link to the organization's homepage, the product or service name, type of product, link to the product homepage, and a notation of the specific point in the CVE Compatibility Process each product or service has reached. Many organizations have multiple products and services listed. For additional usability, they are also listed by product type, product name, organization, and country. Product types include vulnerability databases; security archives and advisories; vulnerability assessment and remediation; intrusion detection, management, monitoring, and response; incident management; data and event correlation; educational materials; and firewalls.

Visit the CVE-Compatible Products and Services page to review information about CVE compatibility, and on all 200 information security products and services.

PredatorWatch, Inc. Makes CVE Compatibility Declarations

PredatorWatch, Inc. has declared that its vulnerability assessment appliance and update service for small to medium enterprises, PredatorWatch Auditor 16 and Update Service; its vulnerability assessment appliance and update service for small mobile networks, PredatorWatch Auditor 128 and Update Service; and its vulnerability assessment appliance and update service for large networks, PredatorWatch Auditor Enterprise and Update Service; are CVE-compatible. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

ThreatGuard, Inc. Makes CVE Compatibility Declaration

ThreatGuard, Inc. has declared that its vulnerability management system, ThreatBox Network Security Appliance, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Backbone Security.com, Inc. Makes CVE Compatibility Declaration

Backbone Security.com, Inc. has declared that its network appliance and managed service, Ribcage 2100, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

October 13, 2004

5-Year Anniversary Q&A with CVE Co-Founder David Mann



David Mann

David Mann Five years ago MITRE Senior Engineer David Mann co-founded CVE with current Editor of the CVE List Steve Christey. Mann left MITRE not long after the public launch of CVE to pursue other opportunities but has since returned, allowing for a unique insider/outsider view of the CVE Initiative.

From a vendor perspective, what's the value of CVE to the information security community?

Mann: At BindView, we really tried to focus on things that would provide a direct business value for our customers. In terms of information security solutions, the business needs that our customers mentioned most often were to decrease their operational costs, manage their IT environment at an acceptable level of risk, and meet their regulatory obligations. CVE clearly delivered on the first of these goals by allowing users to more quickly correlate vulnerability information. By enabling automated data correlation and better clarity for emerging threat information, CVE also enables organizations to do a better job of managing risk. Moving forward, I believe it will be important to clarify how CVE helps with regulatory compliance—for example, FISMA, DISTCAP, HIPAA—which should be easier as CVE grows to cover configuration errors.

What's the biggest difference from what you first imagined for CVE to what it is today?

Mann: By far it is the difficulty in defining what a vulnerability actually is. While CVE identifiers have immediate value for end users, I think one of the big achievements of the effort have been Steve Christey's "Content Decisions", which try to define how to count issues. Perhaps a good analogy is the development of the Dewey Decimal system for organizing and cataloging book. Actually, I think the vulnerability cataloging problem is even harder than dealing with books.

What are your thoughts on the success of CVE within the community, for instance with the number of CVE-compatible products, number of organizations including CVE names in their advisories, and so on?

Mann: It's gratifying, humbling and at times, and frustrating. A mentor once advised me to look for problems, not solutions. CVE was definitely born out of operational pains that Steve and I and others were trying to solve for MITRE's Security Committee. So, when I see CVE numbers in advisories or see the growing list of compatible products, it confirms to me that the problems we were wrestling with were shared by others in the security community. We were just fortunate enough to state the problem in the right forum and context. The idea of assigning unique identifiers quickly took on a life of its own.

The frustrating aspect of this is that the continued growth of CVE is also an indication that the vulnerability management problem is still with us and arguably, continuing to get more complicated and difficult to manage.

Biggest surprise for you from CVE?

Mann: I get surprised every time I see a CVE identifier in print. I still remember a hallway conversation with Jim Williams, who was one of the senior people in my department (and who has since retired) [at MITRE]. I was describing some of the problems that we were running into in our vulnerability management efforts. More accurately, I was ranting and raving about "how things should be" in a more perfect world. Jim told me about a conference that was coming up and encouraged us to write up a paper and to submit it. I mean, he really, really encouraged us.

Now when I see CVE identifiers, I always think of Jim and am reminded of the impact that a mentor can have. It's quite a leap from a hallway rant session to a commonly used standard. Jim easily could have nodded politely and changed the subject. Instead, he invested a bit of time, energy and encouragement and it had very surprising results.

What are your thoughts on the future of CVE?

Mann: The discipline of vulnerability management has been evolving in the past four years and so I think CVE will need to evolve with it. Most obviously, traditional network-based vulnerability assessment has largely been replaced with hybrid solutions that require credentials on the end system being tested. This move goes hand-in-hand with a greater emphasis on configuration settings (called "exposures" in CVE-speak), which require credentialed-based solutions. At the same time, the whole patch management market has emerged, again using credentialed mechanisms with a more narrow focus. Vulnerability management has thus grown to include all three of these: vulnerabilities (software flaws), patches, and configuration management. For CVE to continue its relevance in this larger vulnerability management context, it must grow to

include all three. It's a challenging problem. From a business point of view, I should add that regulatory compliance will continue to refocus vulnerability management efforts more on configuration and patch issues.

Another area of potential growth is the issue of directories. Increasingly, the conceptual objects that security managers need to lock-down aren't defined by the OS. Instead, they are defined by the directory, or worse, by some overlap between the OS and the directory. For example, the concept of "effective rights" tries to define what rights a user has based both on the setting in the OS and on the setting in the domain. This will force CVE to consider the question of moving from OS level vulnerabilities and exposures and to include directory level vulnerabilities. Again, regulatory compliance is going to be a driver in this regard, as it demands that organizations account for what their users can and can't do.

CVE Names Included in Consensus List of "Top Twenty" Internet Security Threats

The recently updated Twenty Most Critical Internet Security Vulnerabilities, a SANS/FBI consensus list of the most critical problem areas in Internet security, was released on October 8, 2004. The list includes CVE names with both entry and candidate status to uniquely identify the vulnerabilities it describes. This will help system administrators use CVE-compatible products and services to help make their networks more secure.

In addition, the introduction page includes a note that describes what CVE is, provides a link to the CVE Web site, and states: "The CVE and CAN numbers reflect the top priority vulnerabilities that should be checked for each item [on the consensus list]."

SANS is a member of the CVE Editorial Board and its education and training materials are listed on the CVE-Compatible Products and Services page.

NetMon2, LLC Makes CVE Compatibility Declaration

NetMon2, LLC has declared that its security information management/security event monitoring (SIM/SEM) product, NetMonSecure, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Senior Advisory Council Holds Meeting

The CVE Senior Advisory Council held a meeting on Wednesday, October 6, 2004. The discussion focused on the two major operational parts of security management; achieving and maintaining secure systems and responding to attacks on our systems and how the CVE and OVAL initiatives have enabled change in each of these processes. The DISA/STRATCOM IA Vulnerability Alert Management (IAVM) Strategy and Contracts were discussed as well as the new consolidated Air Force Microsoft Contract. The requirement for CVE and OVAL is present in each of these contract activities. The current status of the NSA XCCDF (Extensible Configuration Checklist Description Format) effort and the use of OVAL as an external checking method for XCCDF was discussed as well as the integration of OVAL and XCCDF into the CISecurity Tools. Finally, the new DHS/NCSA Common Malware Enumeration (CME) was presented.

The meeting also included status updates on the CVE Initiative, including the recent release of a new version of CVE and upcoming compatible product certificate awards; status updates on the OVAL effort, including a discussion of the working group to discuss modifications to the System Characteristics Schema and OVAL Results Schema.

MITRE established the advisory council to help guide CVE and OVAL and to ensure the initiatives receive appropriate funding, and to help us all understand potential relationships with other ongoing activities, share information, and promote synergy across the security community. The advisory council is composed of senior executives from offices across the U.S. federal government who are responsible for information assurance on government networks and systems. You may also view a list of the advisory council members or read a copy of the council charter.

MITRE to Host CVE/OVAL Booth at CSI's 31st Annual Computer Security Conference and Exhibition

MITRE is scheduled to host a CVE/OVAL exhibitor booth at the Computer Security Institute's (CSI) 31st Annual Computer Security Conference and Exhibition, November 8 - 10, 2004, at the Marriott Wardman Park Hotel, in Washington, D.C., USA. The conference will expose CVE and OVAL to information security and network professionals from industry, academia, and government. In addition, organizations with CVE-Compatible Products and Services will also be exhibiting.

Visit the CVE Calendar page for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

MITRE Hosts CVE/OVAL Booth at SANS Network Security 2004

MITRE hosted a CVE/OVAL exhibitor booth at SANS Network Security 2004, September 30 - October 1, 2004, at the Riviera Hotel in Las Vegas, Nevada, USA. The conference was successful and exposed CVE and OVAL to a diverse audience of network professionals and information security specialists from industry, academia, and government.

Visit the CVE Calendar page for information about this and other upcoming events.

October 4, 2004

Industry Luminaries Discuss 5 Years of CVE

An important aspect of CVE from the outset was cyber security community participation and endorsement. Below are some comments from industry luminaries regarding the value of CVE to the community and the part it has played within the industry these last five years.

"CVE has met and exceeded our expectations. I think it demonstrated its greatest value when it helped foster community-wide consensus on the SANS Top 20 Internet Security Threats."

- Alan Paller, Director of Research, The SANS Institute

"The CVE standard has been, and continues to be, crucial to the effective protection of every organization's critical digital assets. As a founding member of the CVE Editorial Board in 1999 and one of the first organizations to make a declaration of CVE compatibility, ISS congratulates CVE on its five-year anniversary and wishes the initiative ongoing success."

- Peter Allor, Director X-Force Intelligence, Internet Security Systems, Inc.

"The CVE naming standard is an important information security initiative providing a common reference for the entire vulnerability lifecycle including discovery, identification, and remediation of vulnerabilities. As a leading provider of vulnerability management solutions, Qualys has strongly supported CVE since its inception and applauds the MITRE leadership for this critical effort and its value to the security industry as well as our customers."

- Gerhard Eschelbeck, CTO & VP Engineering, Qualys, Inc.

"CVE benefits the community because it provides accurate information on which they can base their security decisions. That is why Red Hat is using the CVE standard in our official 'security roadmap' for Red Hat Enterprise Linux, and why we have so

fully endorsed the initiative by joining the CVE Editorial Board and by making compatibility declarations for our Apache Vulnerability Database and Red Hat Security Advisories. Our security advisories were also recently recognized as one of the first products to be certified officially CVE-compatible. At Red Hat our underlying goal is to advance industry security standards and simplify security for our customers, which is why we will continue to contribute to the CVE group's valuable efforts and congratulate them on their current milestone."

- Mark Cox, Senior Director of Engineering, Red Hat, Inc.

"CVE has enhanced security industry-wide by improving the inter-operability of security products for customers with its common names. Tenable recognizes the importance and value of such standards for end users, which is why three of our products along with Nessus Scanner have CVE compatibility declarations. We believe the continued success of CVE will only be beneficial for our customers."

- Ron Gula, President and CTO, Tenable Network Security, Inc.

In an October 1999 article in Network World magazine about the launch of CVE, Steve Northcutt of SANS said: "... when CVE hits the point of 1,000 entries, it will be a powerful tool." At the five-year mark there are now 7,268 names posted on the CVE site.

"CVE is the standard for identifying vulnerabilities and exposures. With over 7,200 names, nothing else is close. Most of the major tools in the vulnerability space support CVE. The CVE List is a trusted tool for network administrators and security professionals worldwide."

- Steve Northcutt, Director of Training and Certification, The SANS Institute

Grupo S21sec Gestión S.A. Makes CVE Compatibility Declaration

Grupo S21sec Gestión S.A. has declared that its vulnerability notification service and database, Vulnera, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

MITRE to Host CVE/OVAL Booth at FIAC 2004

MITRE is scheduled to host a CVE/OVAL exhibitor booth at Federal Information Assurance Conference (FIAC) 2004, October 26 - 27, 2004, at the Inn and Conference Center, University of Maryland University College, in Adelphi, Maryland, USA. The conference will expose CVE and OVAL to network and systems administrators, security practitioners, acquisition and procurement officials, systems security officers, federal managers, accreditors, and certifiers from numerous agencies of the U.S. federal government. In addition, organizations with CVE-Compatible Products and Services will also be exhibiting.

Visit the CVE Calendar page for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

September 22, 2004

5-Year Anniversary Q&A with CVE Co-Founder Steve Christey



Steve Christey

Five years ago Senior MITRE Information Security Engineer Steve Christey recognized the need for common, standardized vulnerability names and went on to co-found CVE. He now functions as CVE Technical Lead and is Editor of the CVE List.

What's the biggest difference from what you first imagined for CVE to what it is today?

Christey: The first thing that comes to mind is the scale and scope of the effort. In the very beginning, [CVE co-founder] Dave Mann and I just wanted to make it easier to link some tools and advisories together to help with internal MITRE security operations. We were thinking about a couple hundred vulnerabilities from a couple data sources. Now, there are a couple hundred new issues announced PER MONTH, plus we've seen the growth of vulnerability databases, information services, and correlation tools, which barely existed 5 years ago, if at all. And the speed of information exchange is much

faster, too. In hindsight, we were actually kind of provincial in our original view, but then again, we couldn't predict the future. We didn't anticipate that CVE would become a global resource that would apply across a wider variety of tools and information sources. It constantly keeps us on our toes.

What achievement on the project are you most proud of?

Christey: This answer might seem trite, but it's the truth. It's gratifying to know that CVE has helped make many people's jobs easier and, directly or indirectly, help improve the state of information security. This has been demonstrated in many ways over the years. A recent example that comes to mind is the award ceremony for CVE compatible products that we held at the RSA Conference in February 2004. All of the vendors made statements about how CVE had helped them and their customers. Talking with them face-to-face and hearing what they had to say somehow made CVE more "real," which I sometimes forget when I'm just clacking away on the keyboard in my office. Any time people tell us how CVE has helped them is rewarding.

It's also very nice to see large-scale comparisons and trend analyses taking place. These were too resource-intensive to conduct before CVE. This benefit was part of our original vision, but it's only become a reality in the last year or two.

Personally, I'm also proud of being able to share my experiences and knowledge with others in the industry. And I'm proud of the team effort that's gone into CVE, from the contributing individuals in MITRE, to the CVE Editorial Board, to our sponsors over the years, and to all the other community members who've supported it in myriad ways, big and small. CVE is a community-based initiative, and it shows.

Biggest surprise for you working on CVE?

Christey: There have been a few surprises along the way, such as when we started to receive inquiries about CVE compatibility from the marketing directors for security tool vendors. That told us that it wasn't just the technical people who were starting to take CVE seriously. Another surprise occurred when some Linux vendors told me how using CVE had helped them to coordinate bug fixes even before they became public! There are many other surprises, but the biggest one is probably how much CVE has grown and how much it's being used, even in non-English speaking countries.

Surprise, however, is the norm for CVE. We are surprised on a regular basis, and that's a big part of what keeps things interesting, even after 5 years.

Your most difficult challenge working on the project?

Christey: Being all things to all people. As previously mentioned, the scope of CVE is much wider than we had originally anticipated. There are certain sub-communities whose needs could be met by extending CVE in certain ways. We are sensitive to those needs and are doing what we can to address them.

Technically speaking, I think that properly documenting CVE's content decisions—and applying them appropriately—is a significant challenge as well. Vulnerability information is highly volatile, and the quality and quantity of information varies widely and changes over time. This makes it very difficult to be consistent within CVE (and any vulnerability repository faces these challenges, too). CVE's content decisions help to mitigate

these problems, but they are more of a "state of mind" than a pre-canned set of rules. Clearly specified content decisions are my personal albatross.

What's in the future for CVE?

Christey: In the next year, the effort with the widest community impact will involve a single, one-time-only change to the CVE numbering scheme, which will begin sometime in 2005. There are a few reasons for this, but the biggest reason is the fact that the "CAN-yyyy-nnnn" identifier eventually gets changed to a "CVE-yyyy-nnnn" identifier, and this makes for a lot of maintenance headaches and confusion. We are very aware that we can't make this change lightly, and we can only do it once, so we want to do it right and minimize the amount of work required for this one-time change. We're still working on the details, but we expect to announce the specifics soon, and we will be sure to give vendors and consumers plenty of warning before the change takes place.

I previously mentioned certain sub-communities that could be better served by CVE. In the future, we expect to extend CVE (or at least the concept of it) to handle system configuration issues and intrusion detection "events." These are obviously security-relevant, but they don't necessarily fit the concept of "vulnerability" and they don't necessarily translate well into a flat namespace like we've been able to use for vulnerabilities. MITRE's OVAL project is already working in the area of system configuration, but we'd like to have CVE names assigned for the most common issues.

We are also continually working to improve CVE's timeliness and comprehensiveness. Technical CVE users no doubt have noticed our improvements in the past 6 months, but we're going to be even better. Of course, the number of vulnerabilities on the list continues to grow each week, and adding them while maintaining the veracity of what's included in a CVE name is significant work. Soon enough we'll be at 8,000, and it'll keep growing from there.

What else is in the future for CVE? Well, we'll have to wait and see. If there's one thing I've learned on this project, it's to expect the unexpected.

CVE Main Topic of PatchAdvisor, Inc. News Release

CVE was the main topic of a news release by PatchAdvisor, Inc., entitled "PatchAdvisor, Inc. Announces MITRE-CVE Compatibility." The release states: "[PatchAdvisor] has announced that its products are now compatible with MITRE Corporation's Common Vulnerabilities and Exposures ("CVE") dictionary. CVE names are used by information security product/service vendors and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories. Each CVE name includes the following: the CVE identifier number (i.e., "CVE-1999-0067"); indication of "entry" or "candidate" status; brief description of the security vulnerability or exposure; and any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID). "We are very enthusiastic about our inclusion in the CVE compatibility program" says Jeff Fay, PatchAdvisor's CEO. "The ability to standardize the intelligence that we map to our customers' assets is a crucial element in defining PatchAdvisor's role in the vulnerability and patch management market space."

The release also stated: "Visit the CVE-Compatible Products and Services page, <https://cve.mitre.org/>, to find out about the [196] products that use CVE names, or see Organizations with CVE Names in Advisories for a list of the [57] organizations to-date that are including or have included CVE names in their advisories."

PatchAdvisor is listed on the CVE-Compatible Products and Services page.

September 13, 2004

CVE Celebrates 5 Years!

CVE began five years ago this month with 321 entries and 19 information security community organizations participating on an Editorial Board. Since then, CVE has truly become an industry standard. The CVE List has grown to 7,191 total names and the CVE Editorial Board to 35 organizations and 49 members. In addition, more than 120 organizations have made declarations of CVE compatibility for nearly 200 products and services, and 57 organizations are including CVE names in their security advisories.

CVE names are also used on the FBI/SANS Top Twenty List of the Most Critical Internet Security Vulnerabilities list, and on similar threat lists by the Open Web Application Security Project; Internet Security Systems, Inc.; Qualys Inc.; and Sintelli Limited. In 2002, the USA National Institute of Standards and Technology (NIST) released two documents recommending the use of CVE by U.S. agencies: "NIST Special Publication (SP) 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme" and "NIST Special Publication 800-40, Procedures for Handling Security Patches" in which CVE is mentioned throughout. In June 2004, the U.S. Defense Information Systems Agency (DISA) issued a task order for information assurance applications that requires the use of products that use CVE names.

Growth of the CVE List

Initially intended as a source of mature information, the immediate success of CVE names in the community required that the initiative quickly expand to address new security issues that were now appearing almost daily. CVE therefore introduced "candidates," which are CVE names with candidate status. In five short years the CVE List has grown significantly, with approximately 100 new candidates added each month. There are now 7,191 total CVE names on the still growing list, of which 3,052 have official entry status and 4,139 have candidate status.

Growth of CVE-Compatible Products

The information security community endorsed the importance of "CVE-Compatible Products and Services" from the moment CVE was launched in 1999. As quickly as December 2000 there were 29 organizations participating with declarations of compatibility for 43 products. Today, there are 122 organizations and 196 products and services listed on the CVE site. A major milestone for compatibility was the formalization of the CVE Compatibility Process in 2003, ultimately leading to the presentation of "Certificates of CVE Compatibility" in February 2004 to the 10 organizations that achieved official compatibility status for 14 products or services. More than a dozen new products will be certified this fall. CVE names are also included in security advisories from 57 organizations including major OS vendors and others, ensuring that the international community benefits by having CVE names as soon as the problem is announced. And the list of products and advisories continues to grow, with new updates announced regularly on the CVE New and Events page.

CVE has also been used as the basis for entirely new services. NIST's ICAT Metabase, which is a searchable index of vulnerabilities with links to patch information, is built on CVE names. CVE Change Logs is a tool created by CERIAS/Purdue University that monitors additions and changes to the CVE List and allows you to obtain daily or monthly reports. MITRE's Open Vulnerability Assessment Language (OVAL) is the common language for security experts to discuss the technical details of how to identify the presence of vulnerabilities on computer systems using XML definitions that are each based on a CVE name.

Our Anniversary Celebration

It is your participation and endorsement that have transformed CVE into the community standard for vulnerability names. We thank all you who have in any way used CVE names in your products or research, promoted the use of CVE, and/or adopted CVE-compatible products or services for your enterprise. We would also like to thank our sponsors throughout these five years, particularly our current sponsor US-CERT at the U.S. Department of Homeland Security, for their past and current funding and support.

Please join us as our 5-year anniversary celebration continues throughout the month with special news articles on the CVE Web site and culminates with a CVE booth September 29 - October 30 at SANS Network Security 2004, followed by booths at other industry events throughout the fall. We welcome any comments or feedback about CVE.

MITRE to Host CVE/OVAL Booth at SANS Network Security 2004

MITRE is scheduled to host a CVE/OVAL exhibitor booth at SANS Network Security 2004, September 30 - October 1, 2004, at the Riviera Hotel in Las Vegas, Nevada, USA. The conference will expose CVE and OVAL to a diverse audience of network professionals and information security specialists from industry, academia, and government. In addition, organizations with CVE-Compatible Products and Services will also be exhibiting.

Visit the CVE Calendar page for information about this and other upcoming events. Contact us to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

CVE Main Topic of Article in Spanish-Language Security Information and Communications Magazine

CVE was the main topic of an article entitled "CVE and Its Impact on the Management of Vulnerabilities" in the September 2004 issue of Security Information and Communications (SIC) magazine. Written by CVE Compatibility Lead Robert A. Martin, the article describes what CVE is and isn't and explains how vulnerability management can be enhanced using the CVE naming scheme and the adoption of CVE-compatible products and services.

September 1, 2004

New CVE Version Released, Now in XML Format

CVE Version 20040901 has just been released. CVE names are listed with entry or candidate status. 480 new entries have been added, for a total of 3,052 names with official entry status now available. In addition, 4,139 names with candidate status are pending approval by the CVE Editorial Board. This means there are now 7,191 unique information security issues with publicly known names available on the CVE Web site. A report is available to identify the differences between this version and the previous version, 20030402.

CVE names are unique, common identifiers for publicly known information security vulnerabilities. Each CVE name includes the following: the CVE identifier number (i.e., "CVE-1999-0067"); indication of "entry" or "candidate" status; brief description of the security vulnerability or exposure; and any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID). CVE names are used by information security product/service vendors and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE names.

In addition, CVE names are now available in Extensible Markup Language (XML) format. You may download the CVE Entries, CVE Candidates, or All CVE names (entries and candidates) in XML. Support for HTML, text, or comma-separated formats will also continue. CVE is publicly available and free to use. Use Get CVE to view, search, or download CVE.

Computec.ch Makes CVE Compatibility Declaration

Computec.ch has declared that its vulnerability assessment tool, Attack Tool Kit (ATK), is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

August 26, 2004

Eight Organizations Reference CVE Names in Security Advisories

The following eight organizations recently referenced CVE names with entry or candidate (CAN) status in their security advisories: Hong Kong CERT, Indian CERT, French CERT, Poland CERT, Slovenian CERT, OpenSSL, Pine Digital Security, and Netherlands CERT.

- Hong Kong CERT (HKCERT) issued a security advisory in August 18, 2004 that identified CAN-2004-0629. Other advisories also include CVE names.
- Indian CERT (CERT-IN) issued a security advisory in August 11, 2004 that identified CAN-2004-0203. Other advisories also include CVE names.
- French CERT (CERTA) issued a security advisory in August 5, 2004 that identified CAN-2004-0368. Other advisories also include CVE names.
- Poland CERT (CERT Polska) issued a security advisory in August 5, 2004 that identified CAN-2004-0415. Other advisories also include CVE names.
- Slovenian CERT (SI-CERT) issued a security advisory in August 2004 that identified CAN-2004-0549. Other advisories also include CVE names.
- OpenSSL issued a security advisory in March 17, 2004 that identified CAN-2004-0079 and CAN-2004-0112. Other advisories also include CVE names.
- Pine Digital Security issued a security update on February 4, 2004 that identified CAN-2004-0114.
- Netherlands CERT (SURFnet-CERT) issued a security advisory in February 2, 2004 that identified CAN-2003-01025, CAN-2003-01026, and CAN-2003-01027. Other advisories also include CVE names.

See Organizations with CVE Names in Vulnerability Advisories for a complete list of organizations that are including or have included CVE names with entry or candidate status in their security advisories.

August 5, 2004

CVE Included in Article about Early Warnings for CIRT's in Network World Security Newsletter

CVE was mentioned in an article entitled "CIRT management: Rapid alerts" in the July 15, 2004 issue of Network World Fusion's Network World Security Newsletter. The main topic of the article is what the author calls the "three important aspects of early warnings" in Computer Incident Response Team (CIRT) management: "notification of vulnerabilities, notification of threats and notification of incidents."

CVE is included in the "Vulnerabilities" section of the article, in which the author states: "Finally, regular readers will recall that the Common Vulnerabilities and Exposures (CVE) dictionary (<https://cve.mitre.org/>) is a superb compendium of standardized names for vulnerabilities and exposures. MITRE writes, "CVE aspires to describe and name all publicly known facts about computer systems that could allow somebody to violate a reasonable security policy for that system. <https://cve.mitre.org/about/terminology.html>."

The author further states: "MITRE also uses the term "exposure" and defines it as "security-related facts that may not be considered to be vulnerabilities by everyone." You can download the CVE in various formats or you can use the ICAT Metabase (<http://icat.nist.gov/icat.cfm>) to search the CVE for various subsets of vulnerabilities (e.g., by product, version, type, and so on). At the time of this writing (late June) there were 6,663 vulnerabilities in the CVE. As a side note, of these, 1,383 involved buffer overflows (about one-fifth)."

National Institute of Standards and Technology's (NIST) ICAT database is listed on the CVE-Compatible Products and Services page, and NIST is a member of the CVE Editorial Board.

Application Security, Inc. Makes CVE Compatibility Declaration

Application Security, Inc. has declared that its vulnerability assessment tool, AppDetective for Oracle Application Server, is CVE-compatible. In addition, eight other Application Security products are listed on the CVE-Compatible Products and Services page. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

PatchAdvisor, Inc. Makes CVE Compatibility Declaration

PatchAdvisor, Inc. has declared that its patch management tool, PatchAdvisor Enterprise, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Two Organizations Reference CVE Names in Security Advisories

Two organizations recently referenced CVE names with entry or candidate (CAN) status in their security advisories: NoMachine and FedoraNEWS.ORG.

- NoMachine issued a security advisory on March 22, 2004 that identified CAN-2004-0112. Other NoMachine advisories also include CVE names.
- FedoraNEWS.ORG issued a security update on March 3, 2004 that identified CAN-2003-0989, CAN-2004-0057, and CAN-2004-0055. Other FedoraNEWS.ORG updates also include CVE names.

See Organizations with CVE Names in Vulnerability Advisories for a complete list of organizations that are including or have included CVE names with entry or candidate status in their security advisories.

CVE Mentioned in Article about Software Vulnerabilities in Australian Financial Review

CVE was mentioned in an article entitled "Putting a name to evil and its Trojan offspring" in the July 27, 2004 issue of Australian Financial Review. The author states: "CVE serves a number of purposes. The mission statement is to catalogue information technology security risks, allotting a unique identifier to each one. A few years back, the same virus, or Trojan, was often identified by half a dozen different names, depending on which security Web site you visited. Under the CVE regime, each unique species has a registration number. It makes it a lot easier for network administrators to see whether there are 10 threats out there, or 10 variants of a threat, or a single threat with 10 names."

In the article, the author calls CVE a standard and describes what it is; mentions the number of CVE names, including those with entry and those with candidate status; notes that CVE is funded by the U.S. Department of Homeland Security; and provides a link to the CVE Web site.

The article is available for purchase on the Australian Financial Review Web site.

CVE Mentioned in Article about Vulnerabilities on Techworld Web Site

CVE was mentioned in a June 24, 2004 article entitled "Mac OS X security myth exposed — And thousands of other products and OSes given security rundown" on Techworld, the "UK's infrastructure and network knowledge center." CVE is mentioned in a paragraph about three efforts to list known vulnerabilities: "[Secunia Security Advisories database] allows enterprises to gather exact information on specific products, by collating advisories from a large number of third-party security firms. [Other organizations include] the Open Source Vulnerability Database (OSVDB) and the Common Vulnerabilities and Exposures (CVE) [List], which provides common names for publicly known vulnerabilities."

Both the Open Source Vulnerability Database and the Secunia Security Advisories database are listed on the CVE-Compatible Products and Services page.

CVE Names Included in Article on Mac News Network

CVE names were included in a June 7, 2004 article entitled "Apple fixes URI exploits with security update" on the Mac News Network. The article referenced CAN-2004-0538 and CAN-2004-0539, and included links to the pages for these two CVE names on the CVE Web site.

July 15, 2004

7,000+ CVE Names Now Available on the CVE Web Site!

The CVE Web site now contains 7,040 unique information security issues with publicly known names. Of these, 2,572 have CVE entry status and 4,468 have candidate status pending approval by the CVE Editorial Board. CVE names are used by information security product/service vendors and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE names.

CVE names are unique, common identifiers for publicly known information security vulnerabilities. Each CVE name includes the following: the CVE identifier number (i.e., "CVE-1999-0067"); indication of "entry" or "candidate" status; brief description of the security vulnerability or exposure; and any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

Visit the CVE-Compatible Products and Services page to find out about the 193 products that use CVE names, or see Organizations with CVE Names in Advisories for a list of the 47 organizations to-date that are including or have included CVE names in their advisories.

Clear North Technologies Makes CVE Compatibility Declaration

Clear North Technologies has declared that its vulnerability assessment service, Penetration Study, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

CVE Main Topic of Article in Security Horizon Magazine

CVE was the main topic of an article entitled "A CVE-Based Security Management Model" in the Summer 2004 issue of Security Horizon magazine. Written by CVE Compatibility Lead Robert A. Martin, the article describes what CVE is and isn't and explains how vulnerability management can be enhanced using the CVE naming scheme. The article also describes how CVE compatibility enables enterprise security through the use of shared CVE names, and how using CVE-compatible products and services improves how an organization responds to security advisories. A graphical representation of a CVE-enabled process is also included.

July 1, 2004

CVE & OVAL Included as Requirement in U.S. Defense Information Systems Agency Task Order for Information Assurance Applications

CVE and MITRE's Open Vulnerability Assessment Language (OVAL) project were included as requirements in a recent U.S. Defense Information Systems Agency (DISA) task order to DigitalNet, Inc. for information assurance applications. OVAL is the common language for security experts to

discuss the technical details of how to identify the presence of vulnerabilities on computer systems using Community Forum-developed XML definitions, each of which are based on a CVE name.

An article about the task order was published on June 23, 2004 in Government Computer News, which stated: "For the task order, the team will provide the United States Strategic Command with a set of applications that will scan systems for potential vulnerabilities . . . [and] . . . flag incorrect system configurations." According to the task order itself, the "specific CVE and OVAL requirements" are: (1) "Provide a tool for "The ENTERPRISE" to notify their organization of specific vulnerabilities using Common Vulnerability Exposure (CVE) [names] and Open Vulnerability Assessment Language (OVAL) [definitions]," and (2) "Accept configuration and vulnerability-related checking requirements provided by DoD expressed on OVAL eXtensible Markup Language (XML) when available."

In addition, OVAL was referenced in 6.2.3 Subtask 3 - IA Vulnerability Schemes and ODBC Compatibility, which states: "The contractor shall incorporate configuration and vulnerability-related checking requirements provided by DoD expressed in OVAL XML. Being compatible with OVAL means that each tool should be compliant with the "OVAL interface." That interface is described on the OVAL Web site at this URL: http://oval.mitre.org/oval/schema/#XML_format." The subtask further states: "There are XML descriptions (schema) for the OVAL language itself and three platforms currently: Microsoft Windows, Solaris, and Red Hat Linux. These descriptions comprise the OVAL interface. In addition, there are over 500 OVAL definitions for testing vulnerabilities, and a handful of definitions for testing configuration items. It's the interface that's critical for the acquisition."

The Government Computer News article also identifies eEye Digital Security's Retina Network Security Scanner, which scans networks for vulnerabilities, and its REM Security Management Console, a portal for prioritizing vulnerabilities, as part of "the package" to be delivered in the task order. eEye's Retina Network Security Scanner is listed on the CVE-Compatible Products and Services page. You may also read the DigitalNet, Inc. news release, the eEye Digital Security news release, or the DISA task order document.

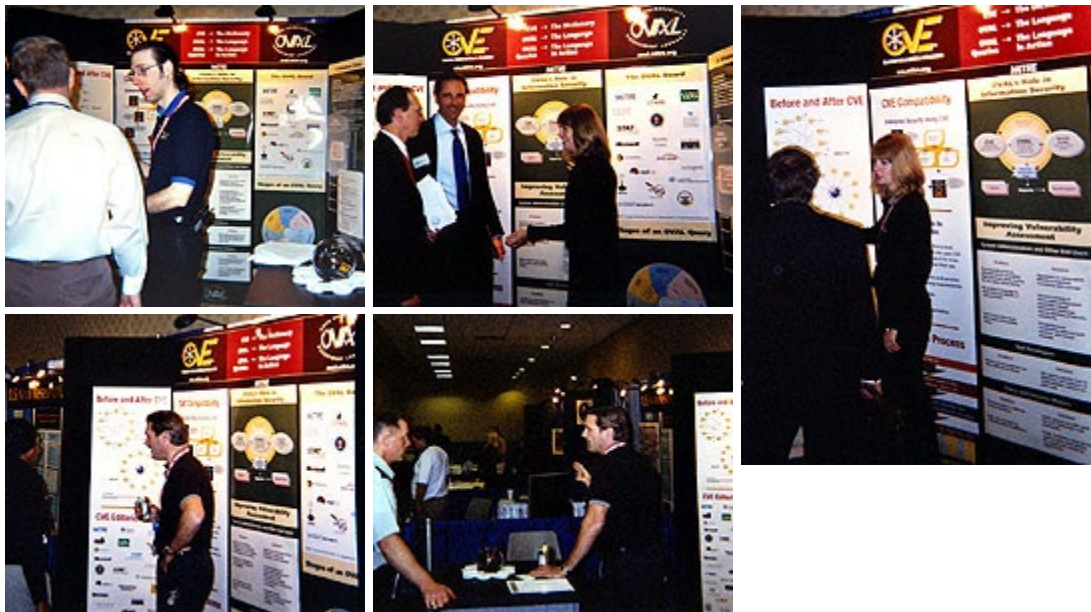
Conference Photos of CVE Booth at Sixth Annual International Techno-Security Conference

MITRE hosted a CVE/OVAL exhibitor booth at the Sixth Annual International Techno-Security Conference June 6th-9th in South Carolina, USA. See photos below.



Conference Photos of CVE Booth at the 2004 Information Assurance Workshop

MITRE hosted a CVE/OVAL exhibitor booth at the 2004 Information Assurance (IA) Workshop February 2nd-4th in Georgia, USA. See photos below.



June 23, 2004

SAINT Corporation Makes CVE Compatibility Declaration

SAINT Corporation has declared that its Web-based vulnerability scanning service, WebSAINT, and its network vulnerability scanning appliance, SAINTbox, are CVE-compatible. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Critical Watch Makes CVE Compatibility Declaration

Critical Watch has declared that its vulnerability assessment and remediation service, PilotVMS, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

AutoProf Makes CVE Compatibility Declaration

AutoProf has declared that its patch management solution, Policy Maker Software Update, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

MITRE Hosts CVE/OVAL Booth at NetSec 2004

MITRE hosted a CVE/OVAL exhibitor booth at NetSec 2004 Conference & Exhibition June 15th - 16th in San Francisco, California, USA. The conference exposed CVE and OVAL to a diverse audience of information security professionals including information security managers and directors; security specialists; systems analysts; network engineers; CIOs and CSOs; network and systems managers and administrators; Web masters; and technical engineers.

Visit the CVE Calendar page for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

June 11, 2004

Trend Micro, Inc. Makes CVE Compatibility Declaration

Trend Micro, Inc. has declared that its vulnerability assessment and remediation product, Trend Micro Vulnerability Assessment, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Security Horizon, Inc. Makes CVE Compatibility Declaration

Security Horizon, Inc. has declared that its National Security Agency INFOSEC Evaluation Methodology (IEM) Certification Course is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

e-Matters References CVE Names in Security Advisories

e-Matters issued a security advisory on June 6, 2004 that identified CAN-2004-0414, CAN-2004-0416, CAN-2004-0417, and CAN-2004-0418. The advisory included a section entitled "CVE Information" that provided brief descriptions of the four CVE names and a link to the CVE Web site. Also included in the section was the following disclaimer: "Please note that only CAN-2004-0416 was discovered by e-Matters." Other e-Matters advisories also include CVE names with entry or candidate (CAN) status in its security advisories.

See Organizations with CVE Names in Vulnerability Advisories for a complete list of organizations that are including or have included CVE names in their security advisories.

'CVE and US-CERT' Page Added to CVE Web Site

A CVE and US-CERT page has been added to the Advisory Council section of the CVE Web site that provides information about the relationship between CVE and US-CERT as well as general information about US-CERT. CVE is sponsored by US-CERT at the U.S. Department of Homeland Security.

CVE Presents Briefing at SecurE-Biz CxO Security Summit

Robert A. Martin, CVE Compatibility Lead and OVAL Team Member, presented a briefing about CVE and OVAL in a discussion session entitled "Standard Building Blocks for Secure Info-Structure" on June 11th at the SecurE-Biz CxO Security Summit in Washington, D.C., USA. The theme of the conference, held June 9th – 11th, was: "Roadmaps for Enabling Secure Information Infrastructure and Cyber Defense".

Visit the CVE Calendar page for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

MITRE Hosts CVE/OVAL Booth at Sixth Annual International Techno-Security Conference

MITRE hosted a CVE/OVAL exhibitor booth at the Sixth Annual International Techno-Security Conference June 6th - 9th in Myrtle Beach, South Carolina, USA. The conference exposed CVE and OVAL to a diverse audience of information security professionals from law enforcement and industry. In addition, CVE Compatibility Lead and OVAL Team Member Robert A. Martin presented a briefing entitled "Managing Vulnerabilities Through Standards" on June 6th.

Visit the CVE Calendar page for information about this and other upcoming events.

May 27, 2004

Tenable Network Security, Inc. Makes CVE Compatibility Declaration

Tenable Network Security, Inc. has declared that its passive vulnerability scanner, NeVO; commercial vulnerability scanner for Windows, NeWT; and its enterprise security management system, Lightning Console; are CVE-compatible. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

StillSecure Makes CVE Compatibility Declaration

StillSecure has declared that its vulnerability assessment and remediation (VAR) system, StillSecure VAM, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

PatchLink Corporation Makes CVE Compatibility Declaration

PatchLink Corporation has declared that its enterprise-wide patch management and vulnerability remediation service, PatchLink Update, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Three Organizations Reference CVE Names in Security Advisories

Three organizations recently referenced CVE names with entry or candidate (CAN) status in their security advisories: Sun Microsystems, AusCERT, and ThaiCERT.

- Sun Microsystems issued a security advisory on May 3, 2004 that identified CAN-2003-0834. Numerous other Sun advisories also include CVE names.
- AusCERT issued a security advisory on May 20, 2004 that identified CAN-2004-0396. Numerous other AusCERT advisories also include CVE names.
- ThaiCERT issued a security advisory in March 2004 that identified CAN-2003-01025, CAN-2003-01026, and CAN-2003-01027. Other ThaiCERT advisories also include CVE names.

See Organizations with CVE Names in Vulnerability Advisories for a complete list of organizations that are including or have included CVE names with entry or candidate status in their security advisories.

CVE Mentioned in Article about OVAL in Security Wire Perspectives

CVE was mentioned in a May 17, 2004 article in Security Wire Perspectives about MITRE's Open Vulnerability Assessment Language (OVAL) project entitled "Security Patches Got You Running in Circles?" Written by CVE Compatibility Lead and OVAL Team Member Robert A. Martin, the article describes what OVAL is and how system administrators would have an easier time managing patches if their vendor's security advisories included OVAL definitions. OVAL is the common language for security experts to discuss the technical details of how to identify the presence of vulnerabilities on computer systems using Community Forum-developed XML definitions, each of which are based on a CVE name.

CVE is mentioned as one of two main reasons for recommending OVAL: "MITRE . . . has developed this initiative to follow the Common Vulnerabilities and Exposures (<https://cve.mitre.org>) model. Where CVE assigns standard names to vulnerabilities, OVAL takes the next step. It's designed to collect and document the latest vulnerability testing ideas, and make them publicly available so that your tool vendors and service providers can incorporate them into the information security products and services you use."

The article also addresses the question of why organizations should adopt OVAL: "It will save your system and security administrator's time, and that translates to lower overhead for you. They can also secure your systems more quickly because they can apply the workarounds and won't have to wait to deploy a patch. Scanning tools will immediately report on successful mitigation, showing the success of any workarounds your system and security administrators have implemented whether or not they applied the patches."

The article also provides link to the CVE and OVAL Web sites.

CVE Compatibility Included as Part of "Security Roadmap" in Press Release by Red Hat, Inc.

CVE compatibility was included in an April 29, 2004 press release by Red Hat, Inc. as one of three facets of Red Hat's "security roadmap." Entitled "Security Takes Lead in Red Hat Enterprise Linux," the press release states that "Since its availability in 2002, Red Hat Enterprise Linux has achieved important milestones in security standards," and includes CVE as item number three: "In February 2004 Red Hat receives MITRE certification for Common Vulnerabilities and Exposures (CVE) compatibility for Security Advisories."

The release also describes how Red Hat security advisories received a certificate of official CVE compatibility: "A second security accomplishment for Red Hat is the certification from MITRE for Common Vulnerabilities and Exposures (CVE) compatibility for Security Advisories. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures to simplify security practices. Red Hat is the only Linux vendor [at this time] to be awarded this certification for security standards."

CVE Compatibility Main Topic of Press Release by Software in the Public Interest, Inc.

CVE compatibility was the main topic of this March 30, 2004 press release entitled "Debian Security Advisories are CVE-Compatible" by Software in the Public Interest, Inc. (SPI). In the release SPI announces that the "Debian Security Advisories (DSA) [were] declared CVE-compatible at the RSA Conference 2004, in San Francisco, February 24th, 2004" during an awards ceremony held at the conference. The release also describes how "The Debian project has added CVE names to all advisories released since September 1998 through a review process started on August 2002. All advisories can be retrieved from the Debian Web site, and announcements related to new vulnerabilities include CVE names if available at the time of their release. Advisories associated with a given CVE name can be searched directly through the [Debian Web site] search engine. Moreover, Debian provides a complete cross-reference table, including all references available for advisories published since 1997. This table is provided to complement the reference map available at CVE."

The release concludes with the following: "Debian developers understand the need to provide accurate and up to date information of the security status of the Debian distribution, allowing users to manage the risk associated with new security vulnerabilities. CVE names enable the project to provide standardised references to all publicly known vulnerabilities and security exposures which allow users to develop a CVE-enabled security management process."

CVE Included as Chapter in Book on Commercial-Off-The-Shelf Based Software Systems

CVE and OVAL were included as a chapter of COTS-Based Software Systems - Third International Conference, ICCBSS 2004 Proceedings, published in April 2004 by Springer-Verlag as part of the Springer-Verlag Lecture Notes in Computer Science. A chapter entitled "Managing Vulnerabilities in Your Commercial-Off-The-Shelf (COTS) Systems Using and Industry Standards Effort (CVE)" was written by CVE Compatibility Lead Robert A. Martin.

May 13, 2004

CVE Topic of Question in Q&A Article about Red Hat Security Response in Wide Open Magazine

CVE was included as a question topic in a question and answer article entitled "Security Response at Red Hat" in the 2004 premiere issue of Red Hat's Wide Open magazine. The article is an interview with Mark Cox, Red Hat Security Response team lead, about how Red Hat deals with security vulnerabilities.

CVE is the topic of the following question: "In Red Hat Security Advisories you refer to CVE names. What are they and why are they useful?" In his answer Cox describes what CVE is and isn't, notes that Red Hat is a member of the CVE Editorial Board, and mentions that the inclusion of CVE names has made Red Hat Security Advisories "more consistent." Cox further states: ". . . all vulnerabilities that have affected Red Hat products from 2000 to date have been given CVE names and all are searchable on [Red Hat's] Web site and in our advisories." The article also includes a screen capture of the CVE Web site showing the CVE name page for CVE-2001-0731.

Red Hat, Inc. is a member of the CVE Editorial Board; is listed on the CVE-Compatible Products/Services page, which includes one product that has been recognized as officially CVE-compatible and awarded a certificate of compatibility; and Red Hat Security Advisories are listed on the Organizations with CVE Names in Advisories page.

MITRE to Host CVE/OVAL Booth at Sixth Annual International Techno-Security Conference

MITRE is scheduled to host a CVE/OVAL exhibitor booth at the Sixth Annual International Techno-Security Conference on June 6th - 9th at the Marriott Resort at Grande Dunes in Myrtle Beach, South Carolina, USA. The conference will expose CVE and OVAL to a diverse audience of information security professionals from law enforcement and industry. In addition, CVE Compatibility Lead and OVAL Team Member Robert A. Martin will present a briefing entitled "Managing Vulnerabilities Through Standards" on June 6th.

Visit the CVE Calendar page for information about this and other upcoming events. Contact us to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

MITRE to Host CVE/OVAL Booth at NetSec 2004 Conference & Exhibition

MITRE is scheduled to host a CVE/OVAL exhibitor booth at NetSec 2004 Conference & Exhibition on June 15th - 16th at the Hyatt Regency Embarcadero in San Francisco, California, USA. The conference will expose CVE and OVAL to a diverse audience of information security professionals including information security managers and directors; security specialists; systems analysts; network engineers; CIOs and CSOs; network and systems managers and administrators; Web masters; and technical engineers. The conference covers "a broad array of topics, including awareness, privacy, policies, wireless security, VPNs, remote access, Internet security and more."

Visit the CVE Calendar page for information on this and other upcoming events.

CVE to Present Briefing at SecurE-Biz CxO Security Summit

Robert A. Martin, CVE Compatibility Lead and OVAL Team Member, is scheduled to present a briefing about CVE and OVAL in a discussion session entitled "Standard Building Blocks for Secure Info-Structure" on June 11th at the SecurE-Biz CxO Security Summit at the Marriott Metro Center in Washington, D.C., USA. The theme of the conference, scheduled for June 9th - 11th, is: "Roadmaps for Enabling Secure Information Infrastructure and Cyber Defense".

Visit the CVE Calendar page for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

CVE and OVAL Included as Chapter in Book on Software Quality Management

CVE and OVAL were included as a chapter of Proceedings of Software Quality Management XII - New Approaches to Software Quality, published in April 2004 by The British Computer Society. A chapter entitled "CVE and OVAL - International Security Standards That Are Making A Difference" was included in "Section 2 - Standards," and was written by CVE Compatibility Lead and OVAL Team Member Robert A. Martin.

CVE Included as Chapter in 5th Edition of Information Security Managers Handbook

CVE was included as chapter in the Information Security Managers Handbook, 5th Edition, published in December 2003 by Auerbach Publications. Chapter 70, entitled "A Progress Report on the CVE Initiative," was written by Steven M. Christey, co-creator and editor of the CVE List; Robert A. Martin, CVE compatibility lead; and David W. Baker, CVE team member. An earlier version of the information provided in this chapter is included on the CVE Documents page.

April 28, 2004

'OVAL XML Reference Interpreter' Finds Vulnerabilities from the CVE Dictionary

MITRE's Open Vulnerability Assessment Language (OVAL) project has released two free Reference XML Definition Interpreters that can determine if a system has vulnerabilities from the CVE dictionary. MITRE developed the Reference Interpreters to demonstrate the usability of OVAL vulnerability definitions, which are gold-standard tests written by the information security community to provide a standardized baseline check for determining the presence of vulnerabilities on end systems. OVAL definitions are based on CVE names; for each name there are one or more definitions.

A Reference Interpreter for Microsoft Windows supports Windows NT 4.0, 2000, XP, and Server 2003, while another supports Red Hat Linux 9 and Red Hat Enterprise Linux 3. The Interpreters are not fully functional scanning tools and have a simplistic user interface, but running one will provide a list of CVE names determined by OVAL to be present on the system. This list is in a format that can easily be incorporated into other information security tools.

Both Interpreters and their associated data files are available for download for free from the OVAL Web site.

CVE the Underpinning for Forrester Research Study

CVE was the underpinning for a Forrester Research study that compared Linux versus Windows in terms of how quickly they fixed security vulnerabilities. The study, which was the topic of a March 30, 2004 article in eWeek entitled "Linux vs. Windows: Which Is More Secure?", would not have been feasible without CVE. It is the first time CVE has been used to support such a large-scale, quantitative analysis. The authors used the National Institute of Standards and Technology's (NIST) ICAT database—which NIST describes as a "CVE Vulnerability Search Engine"—to perform the comparison and to normalize their results. The study is available for purchase on the Forrester Web site.

NIST is a member of the CVE Editorial Board and ICAT is listed on the CVE-Compatible Products and Services page.

CVE Included as a "Best Practice" in Book about E-Business Systems Security

CVE was recommended as a security "best-practice" in a 2002 book entitled Securing E-Business Systems: A Guide for Managers and Executives by Timothy Braithwaite. CVE was discussed in Chapter 4, "Managing E-Business Systems and Security," in which the author provides a thorough description of what CVE is and isn't, describes CVE compatibility, and mentions the CVE Editorial Board. Concluding the discussion, the author states: "Best Practice #12: As a matter of policy, adopt the CVE naming strategy and enforce it's use in all aspects of the e-business security program management."

CVE Presents Briefing at 16th Annual Systems & Software Technology Conference

Robert A. Martin, CVE Compatibility Lead and OVAL Team Member, presented a briefing entitled "Vulnerability Management with Industry Standards (CVE & OVAL)" on April 20th at the 16th Annual Systems & Software Technology Conference at the Salt Palace Convention Center, Salt Lake City, Utah, USA.

The conference, held April 19th - 20th, was co-sponsored by the United States Army, United States Marine Corps, United States Navy, Department of the Navy, United States Air Force, Defense Information Systems Agency (DISA), and Utah State University Extension and aimed to "provide information and training on software engineering issues and technologies" to a wide range of software professionals from the military services, government agencies, defense contractors, industry, and academia.

Visit the CVE Calendar page for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

April 16, 2004

OVAL e-Newsletter Includes CVE Names in Each Issue

The Open Vulnerability Assessment Language (OVAL) project is now offering a free OVAL-Data-Updates e-newsletter that includes CVE names in each issue. Sent once per week or less, OVAL-Data-Updates reports detailed technical information about OVAL including lists of new and modified OVAL vulnerability definitions, all of which are based upon CVE names. A second e-newsletter of general news about OVAL is also available. You may sign-up for either or both mail lists on the OVAL Web site.

The CVE Web site also offers free e-newsletters for CVE news and technical updates. Refer to the Free Newsletters page to sign-up or for additional information.

Beyond Security Ltd. Makes CVE Compatibility Declaration

Beyond Security Ltd. has declared that its Automated Vulnerability Assessment Scanner is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Acrobe Consulting AB Makes CVE Compatibility Declaration

Acrobe Consulting AB has declared that its managed security services, ASM Threat Management and ASM Vulnerability Assessment, are CVE-compatible. For additional information about these and other CVE-compatible products, visit the [CVE-Compatible Products and Services page](#).

Open Source Vulnerability Database (OSVDB) Makes CVE Compatibility Declaration

Open Source Vulnerability Database (OSVDB) has declared that its Open Source Vulnerability Database will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services page](#).

CVE Mentioned in eWeek Article about the Launch of the Open Source Vulnerability Database

CVE was mentioned in an April 12, 2004 article in eWeek magazine entitled "Security Flaws Database Goes Live." The article discusses the recent launch of the free Open Source Vulnerability Database (OSVDB) that is meant to "serve as a central collection point [and resource] for information on any and all security vulnerabilities."

CVE is mentioned at the end of the article when the author states that "[OSVDB] is hoping to begin comparing its database with other similar stores, including the Common Vulnerabilities and Exposures project maintained by The MITRE Corp., so that it can reference [CVE names] wherever they're applicable. The CVE project assigns unique [names] to each new vulnerability and publishes a one-line description of the problem."

Open Source Vulnerability Database also recently declared that its database will be CVE-compatible. See the article above or visit the [CVE-Compatible Products and Services page](#) for additional information.

CVE to Present Briefing at 16th Annual Systems & Software Technology Conference

Robert A. Martin, CVE Compatibility Lead and OVAL Team Member, is scheduled to present a briefing entitled "Vulnerability Management with Industry Standards (CVE & OVAL)" on April 20th at the 16th Annual Systems & Software Technology Conference at the Salt Palace Convention Center, Salt Lake City, Utah, USA.

The conference, to be held April 19th - 20th, aims to "provide information and training on software engineering issues and technologies" to a wide range of software professionals from the military services, government agencies, defense contractors, industry, and academia. The event is co-sponsored by the United States Army, United States Marine Corps, United States Navy, Department of the Navy, United States Air Force, Defense Information Systems Agency (DISA), and Utah State University Extension.

Visit the [CVE Calendar page](#) for information about this and other upcoming events. Contact us to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

CVE Senior Advisory Council Holds Meeting

The CVE Senior Advisory Council held a meeting on Tuesday, April 6, 2004. The meeting included status updates on the CVE Initiative focusing on the recent milestone of 14 products and services from 10 organizations achieving official CVE-compatible status and the CVE compatibility awards ceremony held at RSA 2004; status updates on the OVAL effort, including a discussion of the new XML Reference Definition Interpreters; a discussion of the roles of CVE and OVAL in automating information assurance and vulnerability management; and a presentation by US CERT.

MITRE established the advisory council to help guide CVE and OVAL and to ensure the initiatives receive appropriate funding. The advisory council is composed of senior executives from offices across the U.S. federal government who are responsible for information assurance on government networks and systems. Visit the [Advisory Council section of the CVE Web site](#) to view a list of the advisory council members or to read a copy of the council charter.

CVE Presents Briefing at 12th International British Computer Society Conference on Software Quality Management

Robert A. Martin, CVE Compatibility Lead and OVAL Team Member, presented a briefing entitled "CVE and OVAL—International Security Standards that Are Making a Difference" at the 12th International British Computer Society Conference on Software Quality Management at Christ Church University College, Canterbury, Kent, UK. The conference, held April 5th - 7th, aimed to "promote cooperation and greater understanding [of software quality management] among practitioners and academics by providing an opportunity to share research and practical experience."

Visit the [CVE Calendar page](#) for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about OVAL, CVE, and/or other vulnerability management topics at your event.

March 31, 2004

TruSecure Corporation Makes CVE Compatibility Declaration

TruSecure Corporation has declared that its integrated asset intelligence-based threat management service, TruSecure IntelliShield Early Warning System (EWS), is CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services page](#).

Sourcefire, Inc. Makes CVE Compatibility Declaration

Sourcefire, Inc. has declared that its integrated security monitoring infrastructure for identifying and protecting against network threats, Sourcefire Intelligent Security Monitoring System, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services page](#).

Cubico Solutions CC Makes CVE Compatibility Declaration

Cubico Solutions CC has declared that its continuous risk analysis solution, Foresight, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services page](#).

Skybox Security, Inc. Makes CVE Compatibility Declaration

Skybox Security, Inc. has declared that its exposure risk management solution, Skybox View, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services page](#).

NX Security Makes CVE Compatibility Declaration

NX Security has declared that its vulnerability assessment and remediation services, NX Express and NX Enterprise, are CVE-compatible. For additional information about these and other CVE-compatible products, visit the [CVE-Compatible Products and Services page](#).

Shavlik Technologies, LLC Makes CVE Compatibility Declaration

Shavlik Technologies, LLC has declared that its patch management product, Shavlik Technologies HFNetChkPro, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the [CVE-Compatible Products and Services page](#).

CVE to Present Briefing at 12th International British Computer Society Conference on Software Quality Management

Robert A. Martin, CVE Compatibility Lead and OVAL Team Member, will present a briefing entitled "CVE and OVAL—International Security Standards that Are Making a Difference" at the 12th International British Computer Society Conference on Software Quality Management at Christ Church University College, Canterbury, Kent, UK. The conference, scheduled for April 5th 7th, aims to "promote cooperation and greater understanding [of software quality management] among practitioners and academics by providing an opportunity to share research and practical experience."

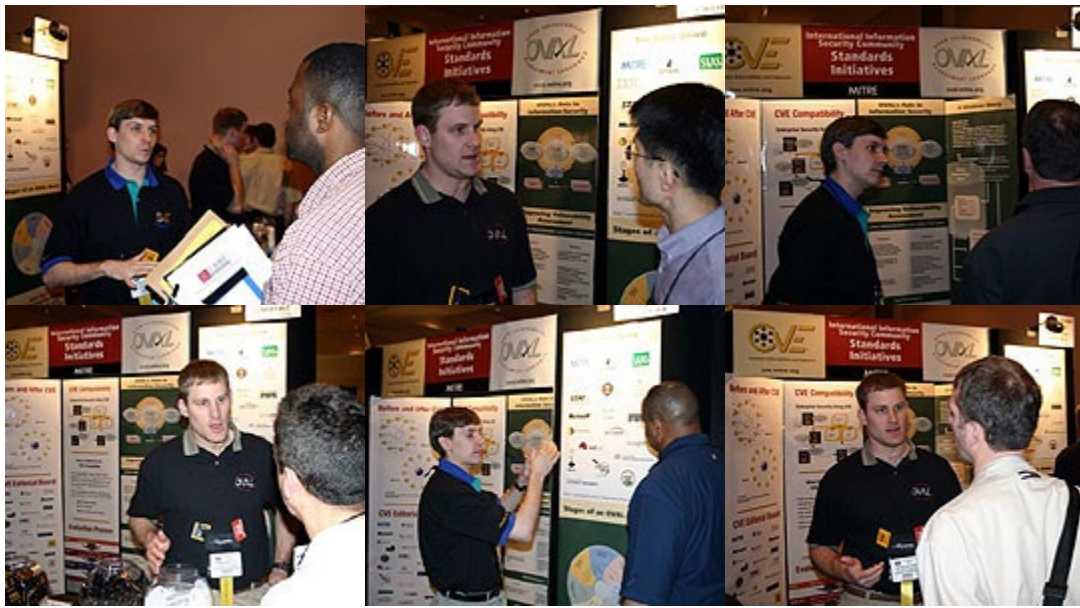
Visit the [CVE Calendar page](#) for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

MITRE Hosts CVE/OVAL Booth at InfoSec World Conference and Expo/2004, March 22nd-24th

MITRE hosted a CVE/OVAL exhibitor booth at MISTI's InfoSec World Conference and Expo/2004 on February 22nd 24th at the Rosen Centre Hotel in Orlando, Florida, USA. The conference was successful and exposed CVE and OVAL to a diverse audience of information security policy and decision makers from the banking, finance, real estate, insurance, and health care industries, among others.

Visit the [CVE Calendar page](#) for information about this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, OVAL, and/or other vulnerability management topics at your event.

See photos below:



Conference Photos of CVE Booth at RSA 2004

MITRE hosted an CVE/OVAL exhibitor booth at RSA Conference 2004 on February 23rd - 27th in San Francisco, California, USA. See photos below.



March 17, 2004

CVE Compatibility Milestone: 100+ Organizations Now Participating!

The CVE Initiative achieved a major milestone with 103 organizations from industry, government, and academia around the world now working to make their products or services CVE-compatible. Sixteen countries are represented, with 167 information security products and services declared CVE-compatible or in the process of being made compatible by these organizations. Of the 167, 14 products/services from 10 organizations have achieved the final phase of MITRE's formal CVE Compatibility Process and are now officially CVE-compatible. These are indicated in the CVE-Compatible Products and Services section of this site with the CVE-Compatible product/service logo.

"CVE-compatible" means that a product or service uses CVE names in a way that allows it to cross-link with other repositories that also use CVE names, as documented in the CVE compatibility requirements. Each item listed on the CVE Web site includes a link to the organization's homepage, the product or service name, type of product, link to the product homepage, and a notation of the specific point in the CVE Compatibility Process each product or service has reached. Many organizations have multiple products and services listed. For additional usability, they are also listed by product type, product name, organization, and country. Product types include vulnerability databases; security

archives and advisories; vulnerability assessment and remediation; intrusion detection, management, monitoring, and response; incident management; data and event correlation; educational materials; and firewalls.

Visit the CVE-Compatible Products and Services page to review information about CVE compatibility, and on all 167 information security products and services.

LURHQ Corporation Makes CVE Compatibility Declaration

LURHQ Corporation has declared that its integrated managed vulnerability scanning service, Managed Vulnerability Assessment, and its security intelligence service, Threat Intelligence, are CVE-compatible. In addition, one other LURHQ Corporation service is listed on the CVE-Compatible Products and Services page. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

KaVaDo Inc. Makes CVE Compatibility Declaration

KaVaDo Inc. has declared that its Web application firewall, InterDo, is CVE-compatible. In addition, one other KaVaDo Inc. product is listed on the CVE-Compatible Products and Services page. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

GuardedNet, Inc. Makes CVE Compatibility Declaration

GuardedNet, Inc. has declared that its enterprise security event management/security information management product, neuSECURE, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

OpenService, Inc. Makes CVE Compatibility Declaration

OpenService, Inc. has declared that its security event management and data/event correlation product, Security Threat Manager (STM), will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

SecureWorks, Inc. Makes CVE Compatibility Declaration

SecureWorks, Inc. has declared that its Network-Based Intrusion Prevention Service, and its Vulnerability Assessment Service, will be CVE-compatible. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Secure Elements, Incorporated Makes CVE Compatibility Declaration

Secure Elements, Incorporated has declared that its automated vulnerability remediation product, Class 5 AVR, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Sandvine Incorporated Makes CVE Compatibility Declaration

Sandvine Incorporated has declared that its service provider network attack traffic monitoring and mitigation system, Worm/DoS Traffic Mitigation (W/DTM), will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

SECNAP Network Security Corporation Makes CVE Compatibility Declaration

SECNAP Network Security Corporation has declared that its managed network security services for precise attack prevention, SECNAP Managed Security Services, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Sunbelt Software, Inc. Makes CVE Compatibility Declaration

Sunbelt Software, Inc. has declared that its vulnerability assessment tool, Sunbelt Network Security Inspector, will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Visionael Corporation Makes CVE Compatibility Declaration

Visionael Corporation has declared that its vulnerability assessment and remediation product, Visionael Security Audit, is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Several Organizations Reference CVE Names in Security Advisories

Four organizations recently referenced CVE names with entry or candidate (CAN) status in their security advisories: Immunix, Inc.; Slackware Linux; The NetBSD Project; and Conectiva Linux.

- Immunix, Inc. issued a security advisory on February 26, 2004 that identified CAN-2004-0077. Numerous other Immunix, Inc. advisories also include CVE names.
- Slackware Linux issued a security advisory on February 13, 2004 that identified CAN-2004-0083, CAN-2004-0084, and CAN-2004-0106. Numerous other Slackware Linux advisories also include CVE names.
- The NetBSD Project issued a security advisory on February 6, 2004 that identified CAN-2004-0114. Numerous other NetBSD Project advisories also include CVE names.
- Conectiva Linux issued a security advisory on March 3, 2003 that identified CAN-2002-1337. Other Conectiva Linux advisories also include CVE names.

See Organizations with CVE Names in Vulnerability Advisories for a complete list of organizations that are including or have included CVE names with entry or candidate status in their security advisories.

March 3, 2004

MITRE Presents CVE Compatibility Certificates in Awards Ceremony at RSA Conference 2004

MITRE held an awards ceremony on Tuesday evening, February 24th at RSA Conference 2004, in San Francisco, California, USA, to present "Certificates of CVE Compatibility" to the 10 organizations that have achieved the final phase of MITRE's formal CVE Compatibility Process and whose 14 information security products or services are now officially "CVE-compatible."

Organizations participating in the ceremony included Foundstone, Inc., Harris Corporation, MITRE Corporation, Qualys, Inc., SAINT Corporation, Sintelli Limited, and Software in the Public Interest, Inc. Organizations receiving certificates but unable to participate in the ceremony were Alliance Qualité Logiciel, Kingnet Security, Inc., and Red Hat, Inc.

RSA '04

MITRE's CVE Compatibility awards ceremony at RSA 2004. Front row, left to right: Rich Brazeau and Christian Nobs, Qualys; Naveed Hamid, Sintelli Limited; Bill Austin, SAINT Corporation. Back row, left to right: Amer Deeba, Qualys; John Payton, US-CERT/DHS; Pete Tasker, MITRE; Gerhard Eschelbeck and Philippe Courtot, Qualys; Bill Wall, Harris Corporation. Not pictured, Dave Cole, Foundstone, Inc.

For additional information about CVE compatibility and to review all products and services listed, visit the CVE Compatibility Process and CVE-Compatible Products and Services pages.

Foundstone, Inc. Issues Press Release Announcing Full CVE Compliance and Receipt of "Certificate of CVE Compatibility"

CVE compatibility was the main topic of a February 25, 2004 press release by Foundstone, Inc. entitled "Foundstone Enterprise Risk Solutions Software Awarded Certificate of Compatibility for Full CVE Compliance." In the release Foundstone announces that its "Foundstone Enterprise Risk Solutions (ERS) vulnerability management software has been named fully compliant with the Common Vulnerabilities and Exposure (CVE) Initiative by The MITRE Corp. The company received its Certificate of Compatibility during an awards ceremony at the 13th Annual RSA Conference in San Francisco."

Also included in the release is a quote by Dave Cole, vice president of product management for Foundstone, who states: "The CVE Initiative was designed to provide security vendors and end-users alike a common language to discover and manage vulnerabilities across diverse security products. By achieving full CVE compatibility, Foundstone has demonstrated its commitment to standards and to ensuring customers have reliable and accurate security data that is interoperable with other security devices, software and services."

RSA '04

Dave Cole, Foundstone, Inc. (right), is presented a Certificate of CVE Compatibility by John Payton, US-CERT/DHS, at MITRE's compatibility awards ceremony at RSA 2004.

Foundstone, Inc. and Foundstone Enterprise Risk Solutions are listed on the CVE-Compatible Products and Services page.

Harris Corporation Issues Press Release Announcing STAT Scanner's Recognition for CVE Compatibility

CVE compatibility was the main topic of a February 26, 2004 press release by Harris Corporation entitled "Harris Corporation's STAT Scanner Product Formally Recognized for Common Vulnerabilities Exposure Compatibility." In the release Harris announces that it "has been formally recognized for Common Vulnerabilities Exposure (CVE) compatibility for [its] STAT Scanner network vulnerability assessment product. The recognition award, presented to Harris this week during the 13th Annual RSA conference in San Francisco, recognizes security products that have incorporated MITRE's CVE listings into their vulnerability search databases."

Also included in the release is a quote by John Payton, Incident Response Manager, National Computer Emergency Readiness Team (US-CERT), Department of Homeland Security, who presented the awards: "This group comes from a pool of nearly 100 organizations that are pursuing CVE compatibility," said Mr. Payton. "We congratulate these recipients, and look forward to seeing more organizations and their products qualify for inclusion in this select group." Harris was one of 10 companies receiving the certificates at the event.

RSA '04

Bill Wall, Harris Corporation (right), is presented a Certificate of CVE Compatibility by John Payton, US-CERT/DHS, at MITRE's compatibility awards ceremony at RSA 2004.

Harris Corporation and STAT Scanner are listed on the CVE-Compatible Products and Services page.

Qualys, Inc. Issues Media Advisory Announcing Receipt of Four Certificates of CVE Compatibility

CVE compatibility was the main topic of a February 24, 2004 media advisory by Qualys, Inc. In the advisory Qualys announces that Certificates of CVE Compatibility were presented during an awards ceremony at the 13th Annual RSA Conference in San Francisco, and that the certificates were presented by John Payton, Incident Response Manager for the National Computer Emergency Readiness Team (US-CERT), Department of Homeland Security.

The advisory also lists the 10 organizations and 14 information security products and services that achieved the final phase of MITRE's formal compatibility process and are now officially "CVE-compatible." Qualys received certificates for four products: QualysGuard Enterprise, QualysGuard Consultant, QualysGuard Express, and QualysGuard MSP.

RSA '04

Amer Deeba, Christian Nobs, Rich Brazeau, and Gerhard Eschelbeck, Qualys (left to right), with their four Certificates of CVE Compatibility that were presented to them by John Payton, US-CERT/DHS, at MITRE's compatibility awards ceremony at RSA 2004.

Qualys, Inc. and QualysGuard Enterprise, QualysGuard Consultant, QualysGuard Express, and QualysGuard MSP are listed on the CVE-Compatible Products and Services page.

SAINT Corporation Issues Press Release Announcing Receipt of "Certificate of CVE Compatibility" for its SAINT Tool

CVE compatibility was the main topic of a February 25, 2004 press release by SAINT Corporation entitled "SAINT Is Certified CVE-Compatible." In the release SAINT announces that "On Tuesday, February 24th, MITRE Corporation awarded their CVE (Common Vulnerabilities and Exposures) Certificate of Compatibility to SAINT5 . . . During an awards ceremony at the 13th Annual RSA Conference in San Francisco, SAINT was honored along side nine other companies out of more than 90 vendors, for their work in this effort and passing the final and most rigorous phase of the compatibility process."

Also included in the release is a quote by Bill Austin, SAINT's Chief Security Officer, who states: "We are delighted that SAINT is being recognized as [an official] CVE-compatible product by The MITRE Corporation. SAINT Corporation recognizes and backs the work of MITRE Corporation and its CVE structure as a significant tool in addressing issues of critical national importance. We have been a supporter of MITRE's CVE project nearly since the beginning. In an expanding sea of vulnerability advisories and tools, we felt that such an initiative would be a great benefit to our customers. Keeping the CVE mapping complete and accurate for SAINT's vulnerability reports and scanning policies has remained a high priority in SAINT's development cycle."

RSA '04

Bill Austin, SAINT Corporation (right), is presented a Certificate of CVE Compatibility by John Payton, US-CERT/DHS, at MITRE's compatibility awards ceremony at RSA 2004.

SAINT Corporation and its Security Administrator's Integrated Network Tool (SAINT) are listed on the CVE-Compatible Products and Services page.

Symantec Corporation Makes CVE Compatibility Declaration

Symantec Corporation has declared that its integrated antivirus, firewall, and intrusion detection service, Symantec Client Security, is CVE-compatible. In addition, Symantec, Inc. is a member of the CVE Editorial Board, and nine other Symantec products are listed on the CVE-Compatible Products and Services page. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

NileSOFT Ltd. Makes CVE Compatibility Declaration

NileSOFT Ltd. has declared that its host-based vulnerability assessment tool, Secuguard System Security Explorer (Secuguard SSE), and its network-based vulnerability assessment tool, Secuguard Network Security Explorer (Secuguard NSE), will be CVE-compatible. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

MITRE to Host CVE/OVAL Booth at InfoSec World Conference and Expo/2004, March 22nd-24th

MITRE is scheduled to host a CVE/OVAL exhibitor booth at MISTI's InfoSec World Conference and Expo/2004 on March 22nd - 24th at the Rosen Centre Hotel in Orlando, Florida, USA. The conference will expose CVE and OVAL to a diverse audience of attendees from the banking, finance, real estate, insurance, and health care industries, among others. The conference is targeted to information security policy and decision makers from these and other industries, as well as directors and managers of information security, CIOs, network and systems security administrators, IT auditors, systems planners and analysts, systems administrators, software and application developers, engineers, systems integrators, strategic planners, and other information security professionals. In addition, numerous companies with CVE-compatible products and services will be exhibiting.

Visit the CVE Calendar page for information on this and other upcoming events.

MITRE Hosts CVE/OVAL Booth at RSA Conference 2004, February 23rd-27th

MITRE hosted a CVE/OVAL exhibitor booth at RSA Conference 2004 on February 23rd - 27th in San Francisco, California, USA. The conference introduced CVE and OVAL to information technology professionals, developers, policy makers, industry leaders, and academics from organizations that deploy, develop, or investigate data security or cryptography products or initiatives. Visit the CVE Calendar page for information about this and other upcoming events.

February 24, 2004

14 Information Security Products/Services Are Now Registered as Officially "CVE-Compatible"

Fourteen information security products and services from ten organizations have achieved the final stage of MITRE's formal CVE Compatibility Process and are now officially "CVE-compatible." Each product is now eligible to use the CVE-Compatible Product/Service logo, and their completed and reviewed "CVE Compatibility Requirements Evaluation" questionnaires are posted as part of their product listings on the CVE-Compatible Products and Services page on the CVE Web site.

The following products are now registered as officially "CVE-Compatible":

Alliance Qualité Logiciel	-	Vigil@nceAQL (Vulnerability Database)
Foundstone, Inc.	-	Foundstone Enterprise 3.0 (Vulnerability Management System)
Harris Corporation	-	STAT Scanner
Kingnet Security, Inc.	-	Kingnet Intrusion Detection System
MITRE Corporation	-	Open Vulnerability Assessment Language (OVAL) Web Site
Qualys, Inc.	-	QualysGuard Consultant
-	-	QualysGuard Enterprise
-	-	QualysGuard Express
-	-	QualysGuard MSP
Red Hat, Inc.	-	Red Hat Security Advisories
SAINT Corporation	-	SAINT (Security Administrator's Integrated Network Tool)
Sintelli Limited	-	Sintelli Alert! (Vulnerability Alert Service)
-	-	Sintelli Vulnerability Database Web Site
Software in the Public Interest, Inc.	-	Debian Security Advisories

Use of the official CVE-Compatible logo by these organizations will allow system administrators and other security professionals to look for the logo when adopting vulnerability management products and services for their enterprises. The compatibility process questionnaires will help end-users compare how different products satisfy the CVE compatibility requirements, and therefore which specific implementations are best for their networks and systems.

An awards ceremony was held tonight in Room 121 North in the Moscone Center at RSA Conference 2004 in San Francisco, California, USA, to present Certificates of CVE Compatibility to the organizations that have achieved this final phase. Organizations participating in the ceremony included Foundstone, Inc., Harris Corporation, MITRE Corporation, Qualys, Inc., SAINT Corporation, Sintelli Limited, and Software in the Public Interest, Inc.

For additional information about CVE compatibility and to review all products and services listed, visit the CVE Compatibility Process and CVE-Compatible Products and Services pages.

Symantec Corporation Makes CVE Compatibility Declarations

Symantec Corporation has declared that its network intrusion detection product, Symantec Vulnerability Assessment, and its intrusion protection product, Symantec iForce IDS Appliance, will be CVE-compatible. In addition, Symantec, Inc. is a member of the CVE Editorial Board,

and eight other Symantec products are listed on the CVE-Compatible Products and Services page. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

MITRE Hosts CVE/OVAL Booth at 2004 Information Assurance Workshop, February 2nd-4th

MITRE hosted a CVE/OVAL exhibitor booth at the 2004 Information Assurance (IA) Workshop in Atlanta, Georgia, USA, February 2nd-4th. The purpose of the workshop, which was hosted by the Defense Information Systems Agency (DISA), National Security Agency (NSA), Joint Staff, and the United States Strategic Commands, was to provide a forum for the IA community on relevant IA topics that have been aligned with the goals of Department of Defense (DOD) IA strategy. The event was successful and introduced CVE and OVAL to representatives of the DOD and other Federal Government employees and their sponsored contractors.

February 11, 2004

MITRE to Host CVE/OVAL Booth at the RSA Conference 2004, February 23rd-27th

MITRE is scheduled to host a CVE/OVAL exhibitor booth at RSA Conference 2004 on February 23rd - 27th in San Francisco, California, USA. The conference will introduce CVE and OVAL to information technology professionals, developers, policy makers, industry leaders, and academics from organizations that deploy, develop, or investigate data security or cryptography products or initiatives.

In addition, 22 organizations listed in the CVE-Compatible Products and Services section are also exhibiting. These organizations are: Application Security, Inc.; ArcSight; Cisco Systems; Citadel Security Software, Inc.; Computer Associates; Enterasys Networks, Inc.; Foundstone, Inc.; IBM; Intellitactics; KaVaDo, Inc.; McAfee Security; nCircle Network Security, Inc.; netForensics, Inc.; NetScreen Technologies, Inc.; Network Box USA, Inc.; NFR Security; Qualys, Inc.; SecurityFocus.com; SPI Dynamics, Inc.; Symantec Corporation; TippingPoint Technologies; and Ubizen, Inc.

Please stop by any of these booths and say hello. Our CVE/OVAL booth number is 1530. We hope to see you there.

Symantec Corporation Makes CVE Compatibility Declaration

Symantec Corporation has declared that its vulnerability alert service and database, DeepSight Alert Services, is CVE-compatible. In addition, Symantec, Inc. is a member of the CVE Editorial Board, and seven other Symantec products are listed on the CVE-Compatible Products and Services page. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Computer Associates International, Inc. Makes CVE Compatibility Declaration

Computer Associates International, Inc. has declared that its vulnerability assessment and remediation vulnerability database product, eTrust Vulnerability Manager, and its vulnerability assessment and remediation product, eTrust Policy Compliance, are CVE-compatible. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Application Security, Inc. Makes CVE Compatibility Declaration

Application Security, Inc. has declared that its vulnerability assessment tool, AppDetective for Web Applications, and its intrusion management and response service, AppRadar for Microsoft SQL Server, are CVE-compatible. In addition, six other Application Security products are listed on the CVE-Compatible Products and Services page. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

NetScreen Technologies, Inc. Makes CVE Compatibility Declaration

NetScreen Technologies, Inc. has declared that its intrusion detection and prevention systems, NetScreen-IDP 10, NetScreen-IDP 500, and NetScreen-IDP 1000, are CVE-compatible. In addition, one other NetScreen Technologies product is listed on the CVE-Compatible Products and Services page. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

InteractNetworks, Inc. Makes CVE Compatibility Declaration

InteractNetworks, Inc. has declared that its commercial appliance-based vulnerability management product, Lockdown Vulnerability Management Appliance (Lockdown VMA), is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

January 23, 2004

CVE Included in InfoWorld Article about Checking Your OS for Vulnerabilities

CVE was included in a January 9, 2004 article entitled "What, me vulnerable? Check your OS for surprises" on the InfoWorld Web site. In the article, the author notes that vulnerabilities exist in most all operating systems (OS), and provides a brief list of some of the more common ones for each. The author also states that while the OS vendors are responsible for offering fixes for vulnerabilities, users also bear some responsibility: "Many serious OS vulnerabilities are the result of poor management, lax administration, or poor configuration. These problems exist for Windows, and they exist for Unix and Linux as well as other operating systems. In addition, some significant vulnerabilities exist in applications that run on top of these operating systems."

CVE is mentioned in the third paragraph, prefacing the brief list of vulnerabilities the author includes in the article: "The following items come from the list available at sans.org and the MITRE Corporation Common Vulnerabilities and Exposures [dictionary]. Both of these sources include information about determining whether or not you're affected by the vulnerabilities." The article also includes a link to the CVE Web site.

January 9, 2004

CVE Is Number 17 in Survey of User's Favorite Security Web Sites by Insecure.org

CVE was listed as number seventeen in a survey of the favorite security Web sites of over 2,000 Insecure.org mailing list subscribers. Of the 153 sites listed in the results, CVE was tied at number seventeen along with astalvista.box.sk, atstake.com, isc.incidents.org, foundstone.com, grc.com, and networkintrusion.co.uk. Of these, FoundStone, Inc. is listed on the CVE-Compatible Products and Services page.

Survey results were posted on December 18, 2003 and can be reviewed on the Insecure.org Web site.

Protego Networks, Inc. Makes CVE Compatibility Declaration

Protego Networks, Inc. has declared that its Mitigation and Response System (MARS) Security Threat Mitigation Appliance will be CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

MITRE to Host CVE Booth at the 2004 Information Assurance Workshop, February 2nd-4th

MITRE is scheduled to host a CVE/OVAL exhibitor booth at the 2004 Information Assurance (IA) Workshop in Atlanta, Georgia, USA, February 2nd - 4th. The purpose of the workshop—which is hosted by the Defense Information Systems Agency (DISA), National Security Agency (NSA), Joint Staff, and the United States Strategic Commands—is to provide a forum in which the IA community can provide updates and work issues on relevant IA topics that have been aligned with the goals of Department of Defense (DOD) IA strategy. The event will introduce CVE and OVAL to representatives of the DOD and other Federal Government employees and their sponsored contractors.

CVE Mentioned in Article about PredatorWatch on Ziff Davis Channel Zone Web Site

CVE was included in a December 24, 2003 article entitled "PredatorWatch Prowls for Network Integrators" on the Ziff Davis Channel Zone Web site. CVE was mentioned in a section of the article entitled "Proving Full Compliance," in which the author states: "That's the idea behind PredatorWatch. Updated daily with a government-sponsored standardized dictionary of vulnerabilities, PredatorWatch generates reports documenting compliance, or areas that need to be looked at. Rather than staffing up to compile its own list of vulnerabilities, PredatorWatch leverages Common Vulnerabilities and Exposures (CVE), a standardized dictionary of known threats. Maintained by MITRE Corp. under a government contract, the CVE dictionary is sold as a subscription [by PredatorWatch], allowing the PredatorWatch Auditor device to automatically update itself daily. The raw CVE dictionary is [free and remains] in the public domain. " The author then goes on to describe how PredatorWatch administers and charges for its CVE updates subscription service.

PredatorWatch, Inc. and PredatorWatch Auditor are listed on the CVE-Compatible Products and Services page.

CVE Mentioned Extensively in Article about TrustSight Security Scanner on the Help Net Security Web Site

CVE and CVE compatibility were mentioned extensively in a January 5, 2004 article entitled "TrustSight Security Scanner Declared CVE-Compatible" on the Help Net Security Web Site. CVE was included in the article title and throughout the text of this article about Syhunt Inf. Ltd.'s, TrustSight Security Scanner. CVE compatibility was referred to in the article subtitle, which reads: "Compatibility Enables Syhunt Customers To Intelligently Analyze, Cross Reference and Search Vulnerabilities". The article itself describes CVE, the CVE Editorial Board, the number of unique and standardized CVE names currently available on the site, and provides a url to the CVE Web site.

The article also quotes CVE Compatibility Lead Robert A. Martin, who states: "[CVE] now includes over 6,400 uniquely named vulnerabilities and more than 200 organizations incorporating CVE names into almost 300 information security products and services. [CVE and CVE compatibility are] making it possible for developers, security practitioners, and systems owners to transform their security practices and make enterprise management of information security vulnerabilities less of an art and more of an engineered practice."

Syhunt, Inf. Ltd. and TrustSight Security Scanner are listed on the CVE-Compatible Products and Services page.

CVE Referred to as a Standard for Vulnerability Names in Network Magazine

CVE was referred to as a standard for vulnerability names in an article about security event management technologies and products entitled "SEM: Navigating the Seas of Security Event Data" in the January 5, 2004 issue of Network Magazine. In a section entitled "Standard Bearers," the author states: "As for identifying vulnerabilities and exposures, MITRE's (www.mitre.org) Common Vulnerabilities and Exposures (CVE) dictionary contains standard names and descriptions of vulnerabilities and exposures."

Of the 19 products discussed in the article, 10 are listed on the CVE-Compatible Products and Services page. This includes five of nine products specifically from security software companies. The 10 organizations and products/services listed in the CVE-Compatible Products and Services section are: IBM's Tivoli Risk Manager, NetIQ's Security Manager, Symantec's Incident Manager, ISS's SiteProtector, Intellitactics's Network Security Manager, netForensics's Security Information Management solution, TruSecure, Symantec's Riptech, and Ubizen.