2007 News — Archive

December 19, 2007

CVE Identifiers Included in Annual Update of "SANS Top Twenty" List of Internet Security Threats

The 2007 Annual Update to the Twenty Most Critical Internet Security Vulnerabilities, a SANS/FBI consensus list of the most critical problem areas in Internet security, was released on November 28, 2007 and now includes 275 CVE Identifiers. The list uses CVE Identifiers to uniquely identify the vulnerabilities it describes. This will help system administrators use CVE-Compatible Products and Services to help make their systems and networks more secure.

The annual update includes six major categories: (1) Client-Side Vulnerabilities in Web Browsers, Office Software, Email Clients, Media Players; (2) Server-Side Vulnerabilities in Web Applications, Windows Services, Unix and Mac OS Services, Backup Software, Anti-virus Software, Management Servers, Database Software; (3) Security Policy and Personnel - Excessive User Rights and Unauthorized Devices, Phishing/Spear Phishing, Unencrypted Laptops and Removable Media; (4) Application Abuse in Instant Messaging and Peer-to-Peer Programs; (5) Network Devices - VoIP Servers and Phones; and (6) Zero Day Attacks.

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

December 5, 2007

CVE Compatibility Requirements Document Updated

The "Requirements and Recommendations for CVE Compatibility" document has been updated to add information aggregators as a new category of tool/service, separate the advisory repositories and vulnerability databases from one category of tool/service into two separate categories, and to update the candidate- and version-related requirements. Comments or questions on these changes are welcome at cve@mitre.org.

MITRE to Host "Making Security Measurable" Booth at 2008 Information Assurance Workshop, January 28 - February 1

MITRE is scheduled to host a Making Security Measurable exhibitor booth at the 2008 Information Assurance Workshop on January 28 - February 1, 2008 at the Philadelphia Marriott Downtown in Philadelphia, Pennsylvania, USA.

The conference will expose the CVE, CCE, CPE, CME, CAPEC, CWE, OVAL, and Making Security Measurable efforts to information security professionals from government and industry. Visit the CVE Calendar for information on this and other events.

November 8, 2007

CVE Mentioned in Article about SCAP in eWeek

CVE was mentioned in an article entitled "SCAP Beta Will Boost Enterprise Compliance Efforts" in eWeek on August 1, 2007. The article describes how the U.S. National Institute of Standards and Technology's Security Content Automation Protocol (SCAP) "…could streamline the way civilian organizations enable automated vulnerability management."

CVE is mentioned when the author states: "SCAP uses data feeds from the NVD (National Vulnerability Database), which is defined and maintained by the National Institute of Standards and Technology, better known as NIST. SCAP is an open standard, and the NVD is available license-free. SCAP uses information from six open standards, including CVE (Common Vulnerability and Exposures) and CCE (Common Configuration Enumeration), both overseen by MITRE, along with data provided by the XCCDF (eXtensible Configuration Checklist Description Format), a standard XML expression for specifying checklists and reporting results from those checklists."

CVE Mentioned in Product Releases Article in Processor Magazine

CVE was mentioned in the "Product Releases" article in Processor Magazine on October 5, 2007. CVE is mentioned in the "Security" section of the article regarding Secure Elements' C5 Compliance Platform 3.3, which "…is the first product to work with NIST SCAP content to help federal government agencies meet the OMB Mandate. It also helps with compliance with NIST ISAP/SCAP initiative for auditing security configurations using OVAL, XCCDF, CPE, CVSS, CCE, and CVE."

CVE Mentioned in Secure Elements Press Release

CVE was mentioned in a September 18, 2007 news release from Secure Elements, Inc. entitled "Secure Elements Announces New Version of IT Audit and Compliance Platform." CVE is mentioned in the portion of the release that describes how Secure Elements' C5 Compliance Platform Version 3.3 adds enhanced NIST SCAP FISMA reporting: "For federal government agencies, C5 is the first enterprise solution that works directly with the NIST SCAP content to help them meet the OMB Mandate for secure desktop configurations as well as incorporating all of the latest standards as defined by the NIST ISAP/SCAP initiative for auditing security configurations utilizing OVAL, XCCDF, CPE, CVSS, CCE and CVE."

Secure Elements, Inc.'s automated vulnerability remediation product, C5 Enterprise Vulnerability Management (EVM) Suite, is listed on the CVE Web site as "Officially CVE-Compatible."

GFI Software Ltd. Posts CVE Compatibility Questionnaire

GFI Software Ltd. has achieved the second phase of the CVE Compatibility Process by submitting a CVE Compatibility Questionnaire for GFI LANguard Network Security Scanner. In Phase 2 of the compatibility process the organization's completed compatibility requirements evaluation questionnaire is posted on the CVE Web site.

October 17, 2007

TecForte Sdn Bhd Posts Two CVE Compatibility Questionnaires

TecForte Sdn Bhd has achieved the second phase of the CVE Compatibility Process by submitting a CVE Compatibility Questionnaire for Log Radar and a CVE Compatibility Questionnaire for LR Assist. In Phase 2 of the compatibility process the organization's completed compatibility requirements evaluation questionnaire is posted on the CVE Web site while it is evaluated by MITRE as the final step towards the product or service being registered as "Officially CVE-Compatible."

For additional information and to review the complete list of all products and services participating in the compatibility program, visit the CVE-Compatible Products and Services section.

AdventNet, Inc. Makes Declaration and Posts CVE Compatibility Questionnaire

AdventNet, Inc. has declared that its vulnerability assessment and remediation product, ManageEngine Security Manager Plus, is CVE-Compatible and has achieved the second phase of the CVE Compatibility Process by submitting a CVE Compatibility Questionnaire for ManageEngine Security Manager Plus. In Phase 2 of the compatibility process the organization's completed compatibility requirements evaluation questionnaire is posted on the CVE Web site while it is evaluated by MITRE as the final step towards the product or service being registered as "Officially CVE-Compatible."

For additional information and to review the complete list of all products and services participating in the compatibility program, visit the CVE-Compatible Products and Services section.

CVE Mentioned in NetworkWorld Article

CVE was mentioned in an article entitled "Service-oriented security" in NetworkWorld on September 25, 2007. CVE is mentioned when the author discusses Security Content Automation Protocol (SCAP). The author states: "The basic premise is that the only way we'll ever get a handle on the operational challenges of security management is to automate as many of the processes as possible. SCAP pulls information from a number of standardized information sources, including (warning: acronym soup ahead): the eXtensible Configuration Checklist Description Format (XCCDF), the Open Vulnerability Assessment Language (OVAL), Common Vulnerability Scoring System, (CVSS) and Common Vulnerabilities and Exposures (CVE) database." The article was written by Andreas M. Antonopoulos.

October 3, 2007

Assuria Limited Posts CVE Compatibility Questionnaire

Assuria Limited has achieved the second phase of the CVE Compatibility Process by submitting a CVE Compatibility Questionnaire for Assuria Auditor (formerly ISS System Scanner). In Phase 2 of the compatibility process the organization's completed compatibility requirements evaluation questionnaire is posted on the CVE Web site while it is evaluated by MITRE as the final step towards the product or service being registered as "Officially CVE-Compatible."

For additional information and to review the complete list of all products and services participating in the compatibility program, visit the CVE-Compatible Products and Services section.

TecForte Sdn Bhd Makes Two Declarations of CVE Compatibility

TecForte Sdn Bhd of Malaysia has declared that its data/event correlation product, Log Radar, and its vulnerability database, LR Assist, are CVE-Compatible. For additional information about this and other CVE-compatible products, visit CVE-Compatible Products and Services.

CVE to Present Briefing at Tactical Information Assurance 2007 on October 26

CVE Compatibility Lead Robert A. Martin is scheduled to present a briefing about CVE/Making Security Measurable at Tactical Information Assurance 2007 on October 26, 2007 at the Georgetown University Conference Center in Washington, D.C., USA.

Visit the CVE Calendar page for information on this and other upcoming events. Contact cve@mitre.org to have CWE present a briefing or participate in a panel discussion about CVE, CCE, CME, CWE, CAPEC, CPE, OVAL, and/or Making Security Measurable at your event.

CVE Included as Topic at Security Automation Conference 2007, September 19-20

CVE was included as a topic at the U.S. National Institute of Standards and Technology's (NIST) Security Automation Conference & Workshop 2007 on September 19-20, 2007 in Gaithersburg, Maryland, USA. NIST's Security Content Automation Protocol (SCAP) employs community standards to enable "automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance)," and CVE is one of the six open standards SCAP uses for enumerating, evaluating, and measuring the impact of software problems and reporting results.

CVE was also a topic in MITRE's Making Security Measurable exhibitor booth during the exhibition portion of the event.The conference exposed the CVE, CCE, CME, CWE, CAPEC, CPE, OVAL, and Making Security Measurable efforts to information security professionals from government and industry.

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

CVE Presents Briefing at ESC Integration Week on September 18th

CVE Compatibility Lead Robert A. Martin presented a briefing about CVE/Making Security Measurable at ESC Integration Week on September 18, 2007 at HANSCOM AFB, Massachusetts, USA.

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

September 12, 2007

GFI Software Ltd. Makes Declaration of CVE Compatibility

GFI Software Ltd. declared that its GFI LANguard Network Security Scanner is CVE-Compatible. For additional information about this and other CVE-compatible products, visit CVE-Compatible Products and Services.

CVE to Present Briefing at ESC Integration Week on September 18th

CVE Compatibility Lead Robert A. Martin is scheduled to present a briefing about CVE/Making Security Measurable at ESC Integration Week on September 18, 2007 at HANSCOM AFB, Massachusetts, USA.

Visit the CVE Calendar page for information on this and other upcoming events. Contact cve@mitre.org to have CWE present a briefing or participate in a panel discussion about CVE, CCE, CPE, CME, CAPEC, CWE, OVAL, and/or Making Security Measurable at your event.

CVE Included in Making Security Measurable Booth at Security Automation Conference 2007, September 19-20

MITRE will host a Making Security Measurable exhibitor booth at the U.S. National Institute of Standards and Technology's (NIST) Security Automation Conference & Workshop 2007 on 19-20, 2007 in Gaithersburg, Maryland, USA. CVE will also participate in discussion panels at the event on September 20th.

NIST's Security Content Automation Protocol (SCAP) employs community standards to enable "automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance)," and CVE is one of the six open standards SCAP uses for enumerating, evaluating, and measuring the impact of software problems and reporting results. The other five standards are Open Vulnerability and Assessment Language (OVAL), a standard XML for security testing procedures and reporting; Common Configuration Enumeration (CCE), standard identifiers and a dictionary for system security configuration issues; Common Platform Enumeration (CPE), standard identifiers and a dictionary for platform and product naming; Extensible Configuration Checklist Description Format (XCCDF), a standard for specifying checklists and reporting results; and Common Vulnerability Scoring System (CVSS), a standard for conveying and scoring the impact of vulnerabilities.

The conference will expose the CVE, CCE, CPE, CME, CAPEC, CWE, OVAL, and Making Security Measurable efforts to information security professionals from government and industry. Visit the CVE Calendar for information on this and other events.

CVE Included in Podcast on BankInfoSecurity.com

CVE Compatibility Lead Robert A. Martin conducted a 10-minute podcast interview with BankInfoSecurity.com about CVE, CWE, and Making Security Measurable at Black Hat Briefings 2007. It is one of nine interviews from the event available at http://www.bankinfosecurity.com/podcasts.php?podcastID=53 (sign-up is required), or you may play or download the podcast now from the CVE Web site.

"Unforgivable Vulnerabilities" Briefing Now Available on CVE Documents Page

CVE Technical Lead Steve Christey presented a "Turbo-Talk" at Black Hat Briefings 2007 on August 2, 2007 entitled "Unforgivable Vulnerabilities." The talk was well-received and had an audience of 80, including several key members of the Web application security community. The briefing is posted for the public on the CVE Documents page.

Contact cve@mitre.org to have CWE present a briefing or participate in a panel discussion about CVE, CCE, CPE, CME, CAPEC, CWE, OVAL, and/or Making Security Measurable at your event.

Photos of Booth at Black Hat Briefings 2007

MITRE hosted a CVE/Making Security Measurable exhibitor booth at Black Hat Briefings 2007 on August 1-2, 2007 at Caesars Palace in Las Vegas, Nevada, USA. See photos below:

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

August 29, 2007

CVE Launches New Web Site

CVE has launched a new CVE Web site that offers more CVE functionality for users through our partnership with the U.S. National Vulnerability Database (NVD), and better illustrates the impact and use of CVE in the community. The updated Web site includes the following enhancements:

- Homepage – in addition to news headlines and a focus on column the homepage now includes a high-level list of examples of the widespread adoption of CVE; a list of similar standards, some of which were inspired by CVE; and a badge indicating that CVE is part of Making Security Measurable.
- CVE in Use page – a new page highlighting how as the international industry standard for vulnerability names CVE Identifiers are included in numerous CVE-Compatible Products and Services, in NVD for fix information for CVE IDs and Security Content Automation Protocol (SCAP) Mappings for CVE IDs, in government, and in the community.
- CVE List Main Page – pointers to the full database functionality for CVE provided through MITRE's partnership with the NVD, and access to the master copy of the CVE List that is maintained for the community by MITRE on this public CVE Web site.
- CVE List page – offers the same view, search, and download features for accessing the master copy of the CVE List as the former Get CVE page.
- Data Updates & RSS Feeds page – pointers to external resources that provide these services for the CVE List.
- Obtain a CVE Identifier page – primarily for vulnerability researchers, this page answers our most frequently asked question: How can I obtain a CVE Identifier?
- About CVE Identifiers page – a new central location for accessing process and technical information about how the CVE project is managed including the method for assigning CVE IDs, role of Candidate Numbering Authorities, content decisions, data sources, reference maps, etc.

CVE Basis of 2007 Edition of "OWASP Top 10 Web Application Security Issues"

The 2007 edition of the "OWASP Top 10 Web Application Security Issues," released on July 17, 2007, is derived entirely from the vulnerability trends detailed in the Vulnerability Type Distributions in CVE white paper by CVE List Editor/Common Weakness Enumeration (CWE) Technical Lead Steve Christey and CWE Program Manager Robert A. Martin. As with previous versions of the OWASP list, the 2007 update also uses CVE Identifiers to identify examples of the vulnerabilities it describes.

OWASP's goal for their Top 10 is to "educate developers, designers, architects and organizations about the consequences of the most common web application security vulnerabilities. The Top 10 provides basic methods to protect against these vulnerabilities – a great start to your secure coding security program."

Integrigy Corporation Makes Declaration of CVE Compatibility

Integrigy Corporation declared that its vulnerability assessment and remediation tool, AppSentry, is CVE-Compatible. For additional information about this and other CVE-compatible products, visit CVE-Compatible Products and Services.

CVE Included as a Topic at Security Automation Conference & Workshop 2007, September 19-20

CVE will be included as a topic at the U.S. National Institute of Standards and Technology's (NIST) Security Automation Conference & Workshop 2007 on September 19-20, 2007 in Gaithersburg, Maryland, USA. In addition to contributing throughout the workshop, CVE will also participate on discussions panels on September 20th.

NIST's Security Content Automation Protocol (SCAP) employs community standards to enable "automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance)," and CVE is one of the six open standards SCAP uses for enumerating, evaluating, and measuring the impact of software problems and reporting results. The other five standards are Open Vulnerability and Assessment Language (OVAL), a standard XML for security testing procedures and reporting; Common Configuration Enumeration (CCE), standard identifiers and a dictionary for system security configuration issues; Common Platform Enumeration (CPE), standard identifiers and a dictionary for platform and product naming; Extensible Configuration Checklist Description Format (XCCDF), a standard for specifying checklists and reporting results; and Common Vulnerability Scoring System (CVSS), a standard for conveying and scoring the impact of vulnerabilities.

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

CVE Mentioned in InfoWorld Article

CVE was mentioned in an August 1, 2007 article entitled "NSA guru lauds security intelligence sharing" in InfoWorld. The main topic of the article was the keynote speech by National Security Agency Vulnerability Analysis and Operations Group Chief Tony Stager at Black Hat Briefings 2007 about how "U.S. government initiatives aimed at fostering the sharing of security intelligence throughout the federal space are helping to establish the community atmosphere and best practices necessary to help those agencies — and private enterprises — improve their network and applications defenses…" that mentioned CVE and the Common Weakness Enumeration (CWE).

CVE is mentioned in the article when the author states: "Robert Martin, head of Mitre's CVE (Common Vulnerability [and] Exposures) compatibility effort and a contributor to the CWE initiative, said that momentum is building behind his organization's guidelines and helping many government and private entities to better understand and share their own practices. "With all these different pieces that are coming together, we are standardizing the basic concepts of security themselves as well as methods for reviewing and improving computing and networking systems," said Martin. "I see a future where a tapestry of tools, procedures, and processes are built over time that recognize and address the common problems that exist among all these constituencies." Martin said that Mitre's efforts to add new security policy frameworks will continue to improve as they mature and even more parties begin to contribute their intelligence to the initiatives."

The article was reprinted in Computerworld on August 2, 2007.

CVE Mentioned in SC Magazine's Vulnerability Assessment 2007 Product Review

CVE was mentioned in a product review group test in SC Magazine entitled "Vulnerability Assessment 2007" that used inclusion of CVE as a review element: "We especially favored those products that take advantage of the common vulnerabilities and exposures (CVE) to define vulnerabilities unambiguously." CVE was also included as a product feature in the individual review for Core Security Technologies' CORE Impact 6.0 automated penetration testing tool.

Core Security Technologies and its CORE Impact 6.0 are listed in the CVE-Compatible Products and Services section.

CVE Included in Booth at Black Hat Briefings 2007

MITRE hosted a Making Security Measurable exhibitor booth at Black Hat Briefings 2007 on August 1-2, 2007 at Caesars Palace in Las Vegas, Nevada, USA. The conference exposed the CVE, CCE, CME, CWE, CPE, OVAL, and Making Security Measurable efforts to a diverse audience of information security-focused attendees from around the world.

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

Common Configuration Enumeration (CCE) Launches Own Web Site

The CCE List is now available on a dedicated Common Configuration Enumeration (CCE) Web site. It will no longer be available on the CVE Web site. The new site includes the CCE List; an Editorial Policies page; an About section describing the overall CCE effort and process in more detail; News page; Calendar page; Community page; and a CCE Working Group page. As CVE provides identifiers for vulnerabilities, CCE provides identifiers for system configuration issues.

July 5, 2007

CVE List Surpasses 25,000+ CVE Identifiers

The CVE Web site now contains 25,064 unique information security issues with publicly known names. CVE, which began in 1999 with just 321 common names on the CVE List, is considered the international standard for public software vulnerability names. Information security professionals and product vendors from around the world use CVE Identifiers (CVE IDs) as a standard method for identifying vulnerabilities, and for cross-linking among products, services, and other repositories that use the identifiers.

The widespread adoption of CVE in enterprise security is illustrated by the numerous CVE-Compatible Products and Services in use throughout industry, government, and academia for vulnerability management, vulnerability alerting, intrusion detection, and patch management. Major OS vendors and other organizations from around the world also include CVE IDs in their security alerts to ensure that the international community benefits by having the identifiers as soon as a problem is announced. CVE IDs are also used to uniquely identify vulnerabilities in public watch lists such as the SANS Top 20 Most Critical Internet Security Vulnerabilities and OWASP Top 10 Web Application Security Issues.

CVE has also inspired new efforts. MITRE's Common Weakness Enumeration (CWE) dictionary of software weakness types is based in part on the CVE List, and its Open Vulnerability and Assessment Language (OVAL) effort uses CVE IDs for its standardized OVAL Vulnerability Definitions that test systems for the presence of CVEs. In addition, the U.S. National Vulnerability Database (NVD) of CVE fix information that is synchronized with and based on the CVE List recently expanded to include Security Content Automation Protocol (SCAP) content. SCAP employs community standards to enable "automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance)," and CVE is one of the six open standards SCAP uses for enumerating, evaluating, and measuring the impact of software problems and reporting results.

Each of the 25,000+ identifiers on the CVE List includes the following: CVE Identifier number (i.e., "CVE-1999-0067"); indication of "entry" or "candidate" status; brief description of the security vulnerability; and pertinent references such as vulnerability reports and advisories or OVAL-ID. Visit the CVE List page to download the complete list in various formats or to look-up an individual identifier. Fix information and enhanced searching of CVE is available from NVD.

Opsware, Inc. Makes Three Declarations of CVE Compatibility

Opsware, Inc. declared that its Internet community portal and subscription service, Opsware Network; its data center automation product, Server Automation System; and its data center automation product, Network Automation System are CVE-Compatible. For additional information about these and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

CVE Included in Booth at Black Hat Briefings 2007

MITRE will host a Making Security Measurable exhibitor booth at Black Hat Briefings 2007 on August 1-2, 2007 at Caesars Palace in Las Vegas, Nevada, USA. The conference will expose the CVE, CCE, CME, CWE, CPE, OVAL, and Making Security Measurable efforts to a diverse audience of information security-focused attendees from around the world.

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

CVE Participates on Discussion Panel at GFIRST Conference

CVE Compatibility Lead Robert A. Martin participated on a discussion panel entitled "Software Assurance (SwA) Panel: Reducing Risk Exposure in the Face Application-Level Threats" at the 3rd Annual GFIRST Conference on June 26, 2007 in Orlando, Florida, USA.

Visit the CVE Calendar page for information on this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, CCE, CME, CWE, CPE, OVAL, and/or Making Security Measurable at your event.

June 22, 2007

SecureInfo Corporation Posts CVE Compatibility Questionnaire

SecureInfo Corporation has achieved the second phase of the CVE Compatibility Process by submitting a CVE Compatibility Questionnaire for SecureInfo RMS. In Phase 2 of the compatibility process the organization's completed compatibility requirements evaluation questionnaire is posted on the CVE Web site while it is evaluated by MITRE as the final step towards the product or service being registered as "Officially CVE-Compatible."

For additional information and to review the complete list of all products and services participating in the compatibility program, visit the CVE-Compatible Products and Services section.

Updated "Common Configuration Enumeration (CCE) List" Posted in CCE Section of CVE Web Site

Version 4.0 of the CCE List has been posted in the "Common Configuration Enumeration (CCE)" section of the CVE Web site. The updated draft focuses on security-related configuration issues for Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Internet Explorer 7, and Office 2007.

CCE provides unique identifiers to system configurations in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. As an example, CCE Identifiers could be used to associate checks in configuration assessment tools with statements in configuration best-practice documents such as the Center for Internet Security (CIS) benchmark documents.

Participation by the information security community is an important element in the success of CCE. We encourage you or your organization to contribute by joining the CCE Working Group or by commenting on the current draft of the CCE List.

CVE Mentioned in Article about Security Content Automation Protocol in Government Computer News

CVE was mentioned in a May 22, 2007 article entitled "NIST releases FISMA security control tools" in Government Computer News. The main topic of the article is the U.S. National Institute of Standards and Technology's Security Content Automation Protocol (SCAP), which according to the article is "intended to help make the step from FISMA compliance to operational IT security." SCAP, an expansion of the U.S. National Vulnerability Database (NVD) that is built upon and synchronized with the CVE List, is an "automated checklist that using a collection of recognized standards for naming software flaws and configuration problems in specific products. It can help test for the presence of vulnerabilities and rank them according to severity of impact. The checklist files are mapped to NIST specifications for compliance with the Federal Information Security Management Act, so that the output can be used to document FISMA compliance."

CVE is mentioned when the author states that "SCAP currently uses six open standards for enumerating, evaluating and measuring the impact of software problems and reporting the results," and includes CVE as the first standard: "Common Vulnerabilities and Exposures, CVE, from MITRE Corp.; standard identifiers and dictionary for security vulnerabilities related to software flaws." The other five standards are: Open Vulnerability and Assessment Language (OVAL), a standard XML for security testing procedures and reporting; Common Configuration Enumeration (CCE), standard identifiers and a dictionary for system security configuration issues; Common Platform Enumeration (CPE), standard identifiers and a dictionary for platform and product naming; Extensible Configuration Checklist Description Format (XCCDF), a standard for specifying checklists and reporting results; and Common Vulnerability Scoring System (CVSS), a standard for conveying and scoring the impact of vulnerabilities.

National Institute of Standards and Technology (NIST) is a member of the CVE Editorial Board and CVE, NVD, and OVAL are all sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security.

CVE to Participate on Discussion Panel at GFIRST Conference

CVE Compatibility Lead Robert A. Martin is scheduled to participate on a discussion panel entitled "Software Assurance (SwA) Panel: Reducing Risk Exposure in the Face Application-Level Threats" at the 3rd Annual GFIRST Conference on June 26, 2007 in Orlando, Florida, USA.

Visit the CVE Calendar page for information on this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, CCE, CME, CWE, CPE, OVAL, and/or Making Security Measurable at your event.

CVE Presents Briefing at System and Software Technology Conference

CVE Compatibility Lead Robert A. Martin presented a briefing about CVE and Making Security Measurable entitled "Creating a Secure Architecture as a Basis for Compliance" at the 19th Annual Systems and Software Technology Conference (SSTC) 2007 on June 20, 2007 in Tampa, Florida, USA.

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

CVE Presents Briefing at Information Assurance Conference of the Pacific

CVE Compatibility Lead Robert A. Martin presented a briefing about CVE and Making Security Measurable at the Information Assurance Conference of the Pacific on June 13, 2007 in Honolulu, Hawaii, USA.

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

June 4, 2007

SecureInfo Corporation Makes Declaration of CVE Compatibility

SecureInfo Corporation declared that its compliance framework tool, SecureInfo RMS, is CVE-Compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Catbird Networks, Inc. Makes Declaration of CVE Compatibility

Catbird Networks, Inc. declared that its hosted security-as-a-service solution for managed service providers, Catbird Shield, is CVE-Compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

SecPoint Makes Declaration of CVE Compatibility

SecPoint declared that its vulnerability assessment and penetration testing appliance, SecPoint Penetrator, will be CVE-Compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

Updated Vulnerability Type Distributions in CVE White Paper Now Available

A May 2007 update to the Vulnerability Type Distributions in CVE has been posted on the CVE Documents page. Originally published in October 2006, this May 22, 2007 update written by CVE List Editor/CWE Technical Lead Steve Christey and CWE Program Manager Robert A. Martin now includes data from all of 2006 and discusses the high-level types of vulnerabilities that have been publicly reported over the past five years, such as buffer overflows, cross-site scripting (XSS), SQL injection, and PHP file inclusion. The paper also identifies and explains trends such as the rapid rise of Web application vulnerabilities, covers the distribution of vulnerability types in operating system vendor advisories, and compares the issues being reported in open and closed source advisories.

CVE Mentioned in Article about the Rate of Vulnerability Disclosures on Dark Reading

CVE was mentioned in a May 30, 2007 article entitled "Bug Disclosures Decline" on Dark Reading. CVE is mentioned at the beginning of the article when the author states: "Researchers say the number of bugs reported so far this year has increased by about 5 percent, versus the 40- to 60-percent spike seen in 2006. Mitre, which officially tracks publicly reported bugs under the Common Vulnerability and Exposures (CVE) program, has seen only a 5 percent increase through April, with 2,245 vulnerabilities reported, versus the 60 percent jump last year at the same time, with 2,143."

The article also includes numerous quotes about the rate of disclosures from CVE List Editor Steve Christey, including that: "In the past couple of years, it seems like there's been a huge increase of independent researchers who use basic techniques to find simple vulnerabilities in software that's not very popular. Maybe we've reached a critical mass in which there are finally enough independent researchers to provide basic evaluations of most software that's available on the Internet." The author also notes that Christey says that there is "typically a sharp increase in bug disclosures when researchers first start working on a new class of products, which typically are loaded with easy-to-find bugs." Christey then continues: "We haven't seen a new product class dominate the landscape since file format vulnerabilities in image or document processing products. There hasn't been a real 'fad' since file-format vulnerabilities, but ActiveX controls show some potential. The numbers could jump again once researchers start hammering away at software that hasn't yet been widely deployed."

The author then concludes the article with a final quote by Christey: "I'm a little surprised [by the rate of vulnerability disclosures so far this year], but after the growth rates of the recent past, there's always hope that the bleeding will slow down. If there's one thing I've learned in this business, it's to expect the unexpected. Numbers ebb and flow all the time."

CVE Presents Briefing at AusCERT 2007

CVE Compatibility Lead/CWE Program Manager Robert A. Martin presented a briefing about CVE and CWE entitled Vulnerability Type Distributions in CVE on May 22, 2007 at AusCERT 2007 at the Royal Pines Resort in Gold Coast, Australia. The presentation is based on the recently updated Vulnerability Type Distributions in CVE white paper (May 22, 2007) that now includes data and analysis for all of 2006.

Visit the CVE Calendar page for information on this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, CCE, CME, CWE, CPE, OVAL, and/or Making Security Measurable at your event.

CVE Presents Briefing to EMC's Software Engineering Workforce

CVE Compatibility Lead/CWE Program Manager Robert A. Martin presented a briefing about CVE and Making Security Measurable to EMC Corporation's Software Engineering Workforce on June 1, 2007 in Hopkinton, Massachusetts, USA.

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

CVE Presents Briefing at Joint Meeting of Boston Software Process Improvement Network/Software Quality Group of New England

CVE Compatibility Lead/CWE Program Manager Robert A. Martin presented a briefing about CVE and Making Security Measurable to the Joint Meeting of Boston Software Process Improvement Network (SPIN) and Software Quality Group of New England (SQNE) session entitled "Exploitable Software: New Security Concerns in a Post-9/11 World" on May 9, 2007 in Burlington, Massachusetts, USA.

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

May 10, 2007

CVE Mentioned in Op-Ed Article about the Importance of Fixing Vulnerabilities in Network World

CVE was mentioned throughout an April 30, 2007 op-ed article entitled "How to find your security holes: Check your network for CVEs" by NetClarity, Inc. founder and CTO Gary S. Miliefsky in Network World. The author, who refers to CVE as a standard and uses the term "CVEs" when referring to vulnerabilities, states that last year alone hackers caused over a billion dollars in damages and that it is "crucial today to prevent vulnerabilities across the enterprise and remove these CVEs - these security holes in your desktops, laptops and servers. Knowing what they are, where they are on your network, and how to remove them is more important than sniffing packets and listening for burglars. According to US-CERT, 95% of downtime and IT related compliance issues are a direct result of an exploit against a CVE."

The author suggests using the SANS Top Twenty consensus list of the most critical software vulnerabilities that are identified by CVE ID to see which vulnerabilities should be fixed immediately and the U.S. National Institute of Standards and Technology's National Vulnerability Database (NVD) that is built upon CVE IDs to search for vulnerabilities and fix information by vendor or OS and product name(s).

The author concludes the article by stating that: "Removing critical CVEs is considered due care. Frequent and consistently scheduled security audits for CVEs and their removal is the only prudent thing to do as a proactive information security manager. Now is the time to find and fix your CVEs so you can be more productive and suffer less downtime and successful hacker attacks. If you remove all of your CVEs you'll be as close to 100% secure as possible."

CVE and NVD are both sponsored by the U.S Department of Homeland Security. Five NetClarity products are listed on the CVE Web site as "Officially CVE-Compatible."

CA References CVE Identifiers in Security Advisories

CA issued a security advisory on April 24, 2007 entitled "[CAID 35277]: CA CleverPath Portal SQL Injection Vulnerability" that referenced CVE-2007-2230. Numerous other CA advisories reference CVE identifiers. To-date, 73 organizations from around the world have included CVE identifiers in their security advisories, ensuring that the community benefits by having CVE identifiers as soon as the problem is announced.

CVE Presents Briefing at MISTI's Government Compliance and Cybersecurity Training Workshop on April 10th

CVE Compatibility Lead Robert A. Martin presented a briefing about CVE and CWE at MISTI's "Government Compliance and Cybersecurity Training Workshop" in Washington, D.C. on April 10, 2007.

Visit the CVE Calendar page for information on this and other upcoming events. Contact cve@mitre.org to have CVE present a briefing or participate in a panel discussion about CVE, CCE, CME, CWE, CPE, OVAL, and/or Making Security Measurable at your event.

April 6, 2007

Two LANDesk Software, Inc. Products Registered as Officially "CVE-Compatible"

LANDesk Software Inc.'s LANDesk Patch Manager and LANDesk Security Suite are the latest to achieve the final stage of MITRE's formal CVE Compatibility Process and are now registered as officially "CVE-compatible." A total of 72 products to-date have been declared officially compatible.

The products are now eligible to use the CVE Compatible logo, and a completed and reviewed "CVE Compatibility Requirements Evaluation" questionnaire is posted for each product as part of the organization's listing on the CVE-Compatible Products and Services page on the CVE Web site. Use of the official CVE-Compatible logo will allow system administrators and other security professionals to look for the logo when adopting vulnerability management products and services for their enterprises and the compatibility process questionnaire 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.

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.

Two AdventNet, Inc. Products Registered as Officially "CVE-Compatible"

AdventNet, Inc.'s SecureCentral PatchQuest and SecureCentral ScanFi are the latest to achieve the final stage of MITRE's formal CVE Compatibility Process and are now registered as officially "CVE-compatible." A total of 72 products to-date have been declared officially compatible.

The products are now eligible to use the CVE Compatible logo, and a completed and reviewed "CVE Compatibility Requirements Evaluation" questionnaire is posted for each product as part of the organization's listing on the CVE-Compatible Products and Services page on the CVE Web site. Use of the official CVE-Compatible logo will allow system administrators and other security professionals to look for the logo when adopting vulnerability management products and services for their enterprises and the compatibility process questionnaire 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.

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.

DEVOTEAM Makes Declaration of CVE Compatibility

DEVOTEAM Solutions - APOGEE declared that its notification service, SECurity Watch Service (offered in French and English), 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 MISTI's Government Compliance and Cybersecurity Training Workshop on April 10th

CVE Compatibility Lead Robert A. Martin is scheduled to present a briefing about CVE and CWE at MISTI's "Government Compliance and Cybersecurity Training Workshop" in Washington, D.C. on April 10, 2007.

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

CVE Mentioned in Article about the Effectiveness of Vulnerability Assessment Tools in Government Computer News

CVE was mentioned in a March 19, 2007 article entitled "All for one, but not one for all" in Government Computer News. The main focus of the article is a National Security Agency (NSA) study of the effectiveness of vulnerability assessment tools, which found that "Organizations trying to automate the process of testing software for vulnerabilities have no choice but to deploy a multitude of tools." The author quotes Kris Britton, technical director at NSA's Center for Assured Software, in describing the results: "No tool stands out as an uber-tool. Each [of the point solution tools] has its strengths and weaknesses."

CVE is mentioned in a discussion about how agreement on what a software weakness is will help the industry in its "quest to find a comprehensive, automated systems analysis of vulnerabilities." The author states: "Mitre Corp. has made some progress on developing a common language for software vulnerabilities, with its initial list of common vulnerabilities and exposures, (CVE) and more recently, the common weakness enumeration (CWE)." He also notes that "CVE includes a list of 20,000 vulnerabilities; CWE includes 600 categories of vulnerabilities." CVE is also mentioned in a quote by Ryan Berg, chief scientist at Ounce Labs, who states: "CVE is a database of vulnerabilities definitions and descriptions [and] CWE is an effort at coming up with a common taxonomy for describing what a particular vulnerability is." CWE, which is based in part on CVE, is mentioned again in a quote by Mike Kass, software assurance project leader at the National Institute of

Standards and Technology, who states that the point of CWE is to "enable more effective discussion, description, selection, and use of software security tools. [Still] There is little overlap among tools regarding what they claim to catch in the CWE. This creates questions for purchasers of tools regarding the tool's purported effectiveness and usefulness." The author also notes that "More than 50 vendors are participating in the [CWE] effort."

CVE Mentioned in Several Articles about SANS's "National Secure Programming Skills Assessment Examination" Initiative

CVE was mentioned in several news media articles about SANS Institute's National Secure Programming Skills Assessment Examination (NSPSA) that will allow government and industrial employers to measure how well their programmers know how to avoid security errors in code they write. The initiative will be piloted this August in Washington D.C., USA and then rolled out worldwide during the remainder of 2007.

The news articles — "SANS: New exam program about more secure code" on TechTarget.com, "Groups team to test secure-coding skill" on SecurityFocus, "Developers' secure-coding skill put to the test" on The Register, "Coalition Aims To Nip Software Bugs In The Bud" on InformationWeek, and "Security Fix: They Say They Want a Revolution" on WashingtonPost.com — quoted from a written statement by CVE List Editor and CWE Technical Lead Steve Christey regarding the need for the exam program: "After reviewing more than 7,000 vulnerabilities in 2006 alone, one thing becomes crystal clear: Most of these vulnerabilities could be found very easily, using techniques that require very little expertise. In my CVE work, I regularly interact with vendors who are surprised to hear of vulnerabilities in their products. They react with the classic stages of shock, denial, anger, bargaining, and finally, acceptance." A second quote used in some of the articles mentions that most colleges and universities don't teach programmers how to write secure code: "There needs to be a revolution. Secure programming examinations will help everyone draw the line in the sand, to say 'No more,' and to set minimum expectations for the everyday developer."

SANS is a member of the CVE Editorial Board, its education and training materials are listed in the CVE-Compatible Products and Services section, and CVE Identifiers are used in its "SANS Top Twenty" list of the most critical Internet security vulnerabilities to uniquely identify the vulnerabilities it describes.

March 29, 2007

Critical Watch Posts Two CVE Compatibility Questionnaires

Critical Watch has achieved the second phase of the CVE Compatibility Process by submitting a CVE Compatibility Questionnaire for FusionVM Managed Service and by making a compatibility declaration and submitting a CVE Compatibility Questionnaire for FusionVM Enterprise System. In Phase 2 of the compatibility process the organization's completed compatibility requirements evaluation questionnaire is posted on the CVE Web site while it is evaluated by MITRE as the final step towards the product or service being registered as "Officially CVE-Compatible."

For additional information and to review the complete list of all products and services participating in the compatibility program, visit the CVE-Compatible Products and Services section.

Security-Database.com Posts CVE Compatibility Questionnaire

Security-Database.com has achieved the second phase of the CVE Compatibility Process by submitting a CVE Compatibility Questionnaire for Security Database Web Site. In Phase 2 of the compatibility process the organization's completed compatibility requirements evaluation questionnaire is posted on the CVE Web site while it is evaluated by MITRE as the final step towards the product or service being registered as "Officially CVE-Compatible."

For additional information and to review the complete list of all products and services participating in the compatibility program, visit the CVE-Compatible Products and Services section.

Lenovo Security Inc. Makes Two Declarations of CVE Compatibility

Lenovo Security Inc. declared that its Leadsec Intrusion Detection System and its Leadsec Intrusion Prevention System are CVE-Compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

CVE Hosts Booth at InfoSec World 2007, March 19-21

CVE co-hosted a Making Security Measurable exhibitor booth at InfoSec World 2007 Conference & Expo on March 19-21, 2007 at the Rosen Shingle Creek Resort in Orlando, Florida, USA. The conference exposed MITRE's CVE, CCE, CME, CWE, CPE, and OVAL efforts 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. Organizations with CVE-Compatible Products and Services also exhibited.

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

CVE Hosts Booth at OMG Software Assurance Workshop, March 5-7

CVE co-hosted a Making Security Measurable exhibitor booth about MITRE's CVE, CCE, CME, CWE, CPE, and OVAL efforts at the OMG Software Assurance Workshop on March 5-7, 2007 at the Hyatt Fair Lakes in Fairfax, Virginia, USA. Object Management Group (OMG) is an international, open membership, not-for-profit computer industry consortium. OMG's task forces "develop enterprise integration standards" for a wide range of technologies and industries and its modeling standards "enable powerful visual design, execution and maintenance of software and other processes."

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

March 2, 2007

CVE Mentioned in Article about Common Weakness Enumeration in CrossTalk Magazine

CVE was mentioned in an article about MITRE's Common Weakness Enumeration (CWE) initiative entitled "Being Explicit About Security Weaknesses" in the March 2007 issue of CrossTalk, The Journal of Defense Engineering. The article describes the creation of the CWE initiative and the sources—including CVE—used to develop the initial concept; related efforts; how CWE is a community effort and a list of current members; how the drafts of the CWE dictionary are being developed; an example of a CWE entry; the CWE Compatibility and CWE Effectiveness program; and the additional impact and transition opportunities tied to CWE.

CVE is mentioned as one of the main sources for the creation of CWE: " ... as part of MITRE's participation in the DHS-sponsored NIST SAMATE effort, MITRE investigated the possibility of leveraging the Common Vulnerabilities and Exposures (CVE) initiative's experience in analyzing more

than 20,000 real-world vulnerabilities reported and discussed by industry and academia. As part of the creation of the CVE List [cve.mitre.org/cve] that is used as the source of vulnerabilities for the National Vulnerability Database [nvd.nist.gov], MITRE's CVE initiative during the last six years has developed a preliminary classification and categorization of vulnerabilities, attacks, faults, and other concepts that can be used to help define this arena."

CVE is mentioned again in the concluding sections as one of the synergies possible from the development of CWE: "Mapping of CWEs to CVEs ... would help bridge the gap between the potential sources of vulnerabilities and examples of their observed instances providing concrete information for better understanding the CWEs and providing some validation of the CWEs themselves." The article was written by CVE Compatibility Lead and CWE Program Manager Robert A. Martin.

Security-Database.com Makes Declaration of CVE Compatibility

Security-Database.com declared that its Security Database Web site is CVE-compatible. For additional information about this and other CVE-compatible products, visit the CVE-Compatible Products and Services page.

CVE to Host Booth at OMG Software Assurance Workshop, March 5-7

CVE is scheduled to co-host a Making Security Measurable exhibitor booth about CVE/CWE/OVAL at the OMG Software Assurance Workshop on March 5-7, 2007 at the Hyatt Fair Lakes in Fairfax, Virginia, USA. Object Management Group (OMG) is an international, open membership, not-for-profit computer industry consortium. OMG's task forces "develop enterprise integration standards" for a wide range of technologies and industries and its modeling standards "enable powerful visual design, execution and maintenance of software and other processes."

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

CVE Mentioned in Article in Network World

CVE was mentioned in a February 2, 2007 article entitled "Inside the X-Force" about IBM Internet Security Systems' X-Force research and development team in Network World. CVE is cited as one of the resources X-Force uses for vulnerability research. The article mentions CVE again when it quotes CVE List editor Steve Christey, who states: "With vulnerability-information management as a discipline, you're taking this mountain of vulnerability data and trying to make it relevant to everyday IT and the security consumer." IBM Internet Security Systems is a member of the CVE Editorial Board and its two X-Force and 5 other products are registered as Officially CVE-Compatible.

CVE Mentioned in Award Description in "2007 SC Magazine Awards"

CVE was cited in the description of SC Magazine's "Editor's Choice Professional Award" to the NSA's Information Assurance Directorate's Vulnerability Analysis and Operations (VAO) Group for its work in the past year with the U.S. Air Force and Microsoft Corporation to "examine and provide security-setting recommendations for Microsoft's new Vista operating system" and to promote the use of standards. CVE was mentioned as follows: "The VAO Group is also shaping the development of security standards for vulnerability naming and identification, such as the Open Vulnerability and Assessment Language (OVAL), Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) standards." The "2007 SC Magazine Awards" were presented on February 6, 2007 at the Hilton San Francisco in San Francisco, California, USA.

Photos from CVE Booth at 2007 Information Assurance Workshop

CVE co-hosted a Making Security Measurable exhibitor booth for MITRE's CVE, CCE, CME, CWE, CPE, and OVAL efforts at the 11th annual 2007 Information Assurance (IA) Workshop on February 12-15, 2007 at the Wyndham Orlando Resort, in Orlando, Florida, USA. See photos below:

February 15, 2007

CVE to Host Booth at InfoSec World 2007, March 19-21

CVE is scheduled to co-host a Making Security Measurable exhibitor booth at InfoSec World 2007 Conference & Expo on March 19-21, 2007 at the Rosen Shingle Creek Resort in Orlando, Florida, USA. The conference will expose MITRE's CVE, CCE, CME, CWE, CPE, and OVAL efforts 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. Organizations with CVE-Compatible Products and Services are also exhibiting.

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

CVE Hosts Booth at 2007 Information Assurance Workshop, February 12-15

MITRE hosted a Making Security Measurable exhibitor booth at the 11th annual 2007 Information Assurance (IA) Workshop on February 12-15, 2007 at the Wyndham Orlando Resort, in Orlando, Florida, USA. The purpose of the workshop, which is hosted by the U.S. Defense Information Systems Agency (DISA) and National Security Agency (NSA), 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 introduced MITRE's CVE, CCE, CME, CWE, CPE, and OVAL efforts to representatives of the DOD and other Federal Government employees and their sponsored contractors. Organizations with CVE-Compatible Products and Services also exhibited.

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

CVE Hosts Booth at RSA Conference 2007, February 5-8

MITRE hosted a Making Security Measurable exhibitor booth at RSA Conference 2007 on February 5-8, 2007 at the Moscone Center in San Francisco, California, USA. RSA Conference provides a forum for information security professionals and visionaries to "exchange and collaborate in a dynamic, authoritative setting." The event introduced MITRE's CVE, CCE, CME, CWE, CPE, and OVAL efforts to security professionals from industry, government, and academia from around the world.

See photos below:








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

CVE Mentioned in Network Security Best Practices Article in Network World

CVE was mentioned in a January 17, 2007 article entitled "The 7 best practices for network security in 2007" in Network World. CVE was mentioned in the third section entitled "Run frequent information security self-assessments," in which the author states: "...Common Vulnerabilities and Exposures (CVE) [is] eight years old this year and accepted worldwide as the de facto international standard for vulnerability tracking on all computers and networking equipment. How many machines on your network have one of the top 20 CVEs? You can find the list here and then find more details at the National Vulnerability Database hosted by NIST."

January 24, 2007

CVE Mentioned in Article about Web Vulnerabilities on CSOonline.com

CVE was mentioned throughout a January 1, 2007 article entitled "The Chilling Effect" on CSOonline.com about "how the Web makes creating software vulnerabilities easier, disclosing them more difficult and discovering them possibly illegal." The author refers to CVE as "the definitive dictionary of all confirmed software bugs."

CVE is mentioned again when the author quotes CVE List Editor Steve Christey on vulnerability disclosure: "Disclosure is one of the main ethical debates in computer security. There are so many perspectives, so many competing interests, that it can be exhausting to try and get some movement forward." The author then uses CVE Identifiers to illustrate responsible disclosure: "Three vulnerabilities that followed the responsible disclosure process recently are CVE-2006-3873, a buffer overflow in an Internet Explorer DLL file; CVE-2006-3961, a buffer overflow in an Active X control in a McAfee product; and CVE-2006-4565, a buffer overflow in the Firefox browser and Thunderbird e-mail program. It's not surprising that all three are buffer overflows. With shrink-wrapped software, buffer overflows have been for years the predominant vulnerability discovered and exploited."

The author also discusses the trends in the types of CVEs: "The speed with which Web vulnerabilities have risen to dominate the vulnerability discussion is startling. Between 2004 and 2006, buffer overflows dropped from the number-one reported class of vulnerability to number four. Counter to that, Web vulnerabilities shot past buffer overflows to take the top three spots. The number-one reported vulnerability, cross-site scripting (XSS) comprised one in five of all CVE-reported bugs in 2006." As part of this discussion the author again quotes Steve Christey: "Every input and every button you can press is a potential place to attack. And because so much data is moving you can lose complete control. Many of these vulnerabilities work by mixing code where you expect to mix it. It creates flexibility but it also creates an opportunity for hacking."

Steve Christey is again quoted in the final section of the article about the future of Web vulnerabilities: "Just as with shrink-wrapped software five years ago, there are no security contacts and response teams for Web vulnerabilities. In some ways, it's the same thing over again. If the dynamic Web follows the same pattern, it will get worse before it gets better, but at least we're not at square one." The author goes on to state that "Christey says his hope rests in part on an efficacious public that demands better software and a more secure Internet, something he says hasn't materialized yet."

CVE Mentioned in Article about Vulnerability Trends on SecurityFocus

CVE was mentioned in a January 17, 2007 article entitled "Vulnerability tallies surged in 2006" on SecurityFocus. The article is about a report on trends in the types of CVEs: "a report released in October by the Common Vulnerabilities and Exposures (CVE) Project found that the top-three categories of flaws were specific to Web programs and accounted for 45 percent of the bugs reported in the first nine months of the year."

The author also includes a quote by CVE List Editor Steve Christey about researchers searching for possible security vulnerabilities: "Many people are doing 'grep and gripe' research. They are doing a regular expression search, looking for patterns. If they get a match they will report it to the public, but sometimes what ends up happening is they are reporting false positives." Christey further states: "You have an emerging levels of sophistication for vulnerability researchers. You have a lot of people who are able to find the low-hanging fruit. But for major software, it seems

to be getting more difficult for top researchers to find these issues--they have to work harder, spend more time, spend more resources, (and) do more complex research."

SecurityFocus is a member of the CVE Editorial Board.

January 5, 2007

CVE Identifiers Included in Annual Update of "SANS Top Twenty" List of Internet Security Threats

The 2006 Annual Update to the Twenty Most Critical Internet Security Vulnerabilities, a SANS/FBI consensus list of the most critical problem areas in Internet security, was released on November 15, 2006 and now includes 210 CVE Identifiers. The list uses CVE Identifiers 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.

The annual update includes five major categories: (1) Operating Systems - Internet Explorer, Windows Libraries, Microsoft Office, Windows Services, Windows Configuration Weaknesses, Mac OS X, and UNIX Configuration Weaknesses; (2) Cross-Platform Applications - Web Applications, Database Software, P2P File Sharing Applications, Instant Messaging, Media Players, DNS Servers, Backup Software, and Security, Enterprise, and Directory Management Servers; (3) Network Devices - VoIP Servers and Phones, and Network and Other Devices Common Configuration Weaknesses; (4) Security Policy and Personnel - H1. Excessive User Rights and Unauthorized Devices, and Users (Phishing/Spear Phishing); and (5) a Special Section - Zero Day Attacks and Prevention Strategies.

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

CVE to Host Booth at RSA Conference 2007, February 5-8

MITRE is scheduled to host a CVE/CCE/CME/CWE/OVAL exhibitor booth at RSA Conference 2007 on February 5-8, 2007 at the Moscone Center in San Francisco, California, USA. RSA Conference provides a forum for information security professionals and visionaries to "exchange and collaborate in a dynamic, authoritative setting." The event will introduce CVE, CCE, CME, CWE, and OVAL to security professionals from industry, government, and academia from around the world. Organizations with CVE-Compatible Products and Services will also be exhibiting. Please stop by Booth 1949, or any of these booths, and say hello.

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

CVE to Host Booth at the 2007 Information Assurance Workshop, February 12-16

MITRE is scheduled to host a CVE/CCE/CME/CWE/OVAL exhibitor booth at the 11th annual 2007 Information Assurance (IA) Workshop on February 12-16, 2007 at the Wyndham Orlando Resort, in Orlando, Florida, USA. The purpose of the workshop, which is hosted by the U.S. Defense Information Systems Agency (DISA) and National Security Agency (NSA), 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, CCE, CME, CWE, and OVAL to representatives of the DOD and other Federal Government employees and their sponsored contractors. Organizations with CVE-Compatible Products and Services will also be exhibiting.

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

CVE Included in Article about Web Application Vulnerabilities in SC Magazine

CVE was mentioned in a December 27, 2006 article entitled "Hot or Not: Web Application Vulnerabilities" in SC Magazine. The article is about a report on trends in the types of CVEs: "There's no doubt that web applications have become the attackers' target of choice. In September, Mitre Corp.'s Common Vulnerabilities and Exposures list - a tally of publicly disclosed vulnerabilities - ranked cross-site scripting in the number one slot. In fact, cross-site scripting attacks surpassed buffer overflow vulnerabilities. And four of the top five reported vulnerabilities proved to be within web applications."

The article also mentions that in the November 2006 SANS Institute Top-20 Internet Security Attack Targets 2006 Annual Update, which uses 210 CVE Identifiers to uniquely identify the vulnerabilities it describes, "web applications topped the list for Cross-Platform Application vulnerabilities."