See the latest News & More

CVE Program Press Releases Archive

The CVE Program issued nine (9) press releases during the period of 1999 – 2019. Those 9 press releases are included below for historical purposes.

September 2014

FOR IMMEDIATE RELEASE

Leading Software Vendors and Cybersecurity Organizations Among Early Adopters of MITRE's New Vulnerability Naming Format

MCLEAN, Va., September 17, 2014—The MITRE Corporation has announced that several leading software vendors and cybersecurity organizations are now consuming or producing Common Vulnerabilities and Exposures (CVE®) Identifier numbers—also called "CVE-IDs"—in the new numbering format. By taking this important step, these organizations ensure that their products, tools, and processes that use CVE will continue to work properly once CVE-ID numbers are issued using the new syntax, which could happen before the end of 2014, and no later than Tuesday, January 13, 2015. CVE is the worldwide standard for information security vulnerability names, and the CVE List provides a dictionary of common names for publicly known information security vulnerabilities in software. MITRE operates CVE on behalf of and with the sponsorship of US-CERT in the office of Cybersecurity and Communications in the U.S. Department of Homeland Security.

The syntax of CVE-ID numbers (e.g., CVE-2014-0160, which had four digits at the end) was changed in January 2014 to accommodate five, six, or more end digits so that CVE can track 10,000 or more vulnerabilities for a given calendar year. The previous four-digit restriction only allowed up to 9,999 vulnerabilities per year, but a change was needed to keep pace with the growing number of vulnerabilities being reported annually. It is possible that 10,000 CVE-IDs will be necessary before the end of 2014.

If the format change is not implemented in a timely manner, it could significantly impact CVE users' vulnerability management practices. To encourage industry and other CVE users to accommodate the new format, MITRE is recognizing those organizations that have declared that they are, or will be, compliant with the new CVE-ID numbering format.

Early adopters of the new CVE-ID format include: Adobe; CERIAS at Purdue University; CERT Coordination Center (CERT/CC); CERT-IST; EMC Corporation; High-Tech Bridge SA; IBM; ICS-CERT; Information-technology Promotion Agency, Japan (IPA); Japan Computer Emergency Response Team Coordination Center (JPCERT/CC); LP3; Microsoft Corporation; National Institute of Standards and Technology, National Vulnerability Database (NVD); NSFOCUS; Oracle; Red Hat, Inc.; SecurityTracker; SUSE LLC; and Symantec Corporation.

"We are assigning new CVE-IDs at an unprecedented rate," said Steve Christey Coley, principal information security engineer at MITRE and editor of the CVE List. "It's too close to call right now, but we could exceed the four-digit limit before the end of this year. If we need more than 9,999 CVE-IDs in 2014, we will follow the new syntax and start using five-digit CVE-IDs. If organizations don't update to the new CVE-ID format, their products and services could break or report inaccurate vulnerability identifiers, making vulnerability management more difficult. To make it easy to update, we have added a section on the CVE website that provides free technical guidance and test data for developers and consumers to use to verify that their products and services will work correctly."

The CVE dictionary contains more than 63,000 unique entries. Products, services and organizations around the world use CVE-IDs to help enhance information security, and CVE is formally recommended by the International Telecommunication Union (ITU-T) standards body for worldwide use.
"The clock is ticking," added Steve Boyle, principal information security engineer at MITRE and CVE program manager. "Even if we don't have to move to the new syntax before the end of 2014, we will ensure that we issue at least one five-digit CVE-ID by Tuesday, January 13, 2015. All organizations that use CVE-IDs need to take action now to make the upgrade before this rapidly-approaching deadline."
About The MITRE Corporation

About the MITRE Corporation
The MITRE Corporation is a not-for-profit organization that operates research and development centers sponsored by the federal government. Learn more about MITRE.

December 2013

FOR IMMEDIATE RELEASE

CVE Vulnerability Dictionary to Adopt the Common Vulnerability Reporting Framework (CVRF) Standard

MCLEAN, Va., December 9, 2013—The MITRE Corporation announced today that the Common Vulnerabilities and Exposures (CVE®) List will now publish data using the Common Vulnerability Reporting Framework (CVRF). The CVE List is a dictionary of common names for publicly known information security vulnerabilities in software.

"Presenting the CVE List in CVRF format will make it easier for people to access CVE content instead of having to use our custom format," said Steve Christey Coley, principal information security engineer at MITRE and editor of the CVE List. "We hope this will encourage others in the security community to share vulnerability information using a standardized machine-readable format."

Developed by the Industry Consortium for Advancement of Security on the Internet (ICASI), CVRF is an XML-based standard that enables software vulnerability information to be shared in a machine-parsable format between vulnerability information providers and consumers. Having vulnerability information in a single, standardized format speeds up information exchange and digestion, while also enabling automation. CVRF is currently used by major vendors, including Red Hat, Microsoft, Cisco Systems and Oracle Corporation, which issue their security advisories in CVRF format:

- Mark Cox, senior director of Product Security at Red Hat: "Red Hat provides CVRF representations of our security advisories and we make heavy use of data provided by the MITRE CVE project. Having their data in a common standard format will help us and others consume it."
- Dustin Childs, group manager of Microsoft Trustworthy Computing: "Customer protection is a priority for Microsoft, and adoption of the new standardized CVRF format extends customer access to crucial information about CVEs. We are pleased to support an advance that makes it easier to understand and address vulnerabilities."
- Mike Schiffman, applied researcher, Cisco Systems and ICASI CVRF Working Group chair:"Cisco, a founding member of ICASI and CVRF working group chair, is happy to help MITRE deploy the de-facto standard for the automated creation and consumption of machine-readable vulnerability documentation."
- Mary Ann Davidson, chief security officer for Oracle Corporation: "Oracle has been publishing CVRF since early 2012 for all vulnerability communications. We are delighted that MITRE will be providing CVE information in CVRF format, as it will further enable the sharing of security information in a machine-readable format, thus allowing organizations to more quickly and efficiently react when security vulnerability information is published."

The CVE dictionary, sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security (DHS), contains more than 58,000 unique entries and is considered an international standard. Products, services and organizations around the world use CVE-IDs to help enhance information security, and CVE is formally recommended by the International Telecommunication Union (ITU-T) standards body for worldwide use.

"Because vulnerability information comes from many diverse sources, a common format makes it easier to analyze and import data without having to create custom tools or to do so manually," added Christey. "Encouraging the use of CVRF means CVE and other vulnerability information consumers can reduce the effort needed to support the wide variety of formats currently in use. And because of its adoption by major vendors, CVRF has a better chance of success compared to earlier efforts, particularly as the need grows for automated exchange of vulnerability data."

About The MITRE Corporation

The MITRE Corporation is a not-for-profit organization that operates research and development centers sponsored by the federal government. Learn more about MITRE.

October 2009

FOR IMMEDIATE RELEASE

MITRE Celebrates a Decade of Software Security with CVE

BEDFORD, Mass., October 21, 2009 — The MITRE Corporation announced the 10th anniversary of the launch of the Common Vulnerabilities and Exposures dictionary, which provides researchers, software vendors, the security community, and end users with a global naming standard for identifying and sharing information about publicly known security vulnerabilities in software products.

The CVE database now contains more than 38,000 entries, each corresponding to a unique publicly known information security issue in a software product. Since its launch in 1999, users in government, industry, and academia have adopted CVE across the world as the authoritative source of data about critical software flaws. As an international information security effort, CVE continues to evolve through the input of experts at MITRE, its government sponsors, software vendors, and researchers.

"CVE is a great example of how MITRE has worked across agencies and among industry, government, and academia to foster advances in cybersecurity that support the national interest," said Robert Nesbit, senior vice president and general manager of MITRE's Center for Integrated Intelligence Systems.

A large variety of CVE-compatible products and services are used throughout industry and government agencies, and among researchers. These products and services address vulnerability management and alerts, intrusion detection, and patch management. In addition, CVE identifiers have been included in security advisories from 73 organizations, including major operating systems vendors.

The success of CVE and the other efforts it has inspired, including the U.S. National Vulnerability Database operated by the National Institute of Standards and Technology (NIST), eventually enabled the creation of NIST's Security Content Automation Protocol, or SCAP. As part of overall efforts over the last 10 years to help the security community produce automated standardized benchmarks, MITRE has developed four of the six security standards which comprise SCAP.

The four standards are:

- Common Vulnerabilities and Exposures (CVE®)
- Open Vulnerability and Assessment Language (OVAL®)
- Common Platform Enumeration (CPE™)
- Common Configuration Enumeration (CCE™)

CVE is used by SCAP for enumerating, evaluating, and measuring the impact of software problems. In addition, CVE is a requirement in U.S. Department of Defense contracts for vulnerability management capabilities.

About The MITRE Corporation
The MITRE Corporation (www.mitre.org) is a not-for-profit organization that provides systems engineering, research and development, and information technology support to the government. It operates federally funded research and development centers for the Department of Defense, the Federal Aviation Administration, the Internal Revenue Service and Department of Veterans Affairs, and the Department of Homeland Security, with principal locations in Bedford, Mass., and McLean, Va.

December 2002

FOR IMMEDIATE RELEASE

MITRE Announces New Standard for Computer Vulnerability Assessment

Bedford, MA, December 10, 2002 — The MITRE Corporation announced today the availability of Open Vulnerability Assessment Language (OVAL), a new community-wide standard for how computer vulnerabilities are identified on local systems.

Computer vulnerabilities are the entry points for hackers, and if not fixed can result in significant recovery expenses in the event of a compromise. A preview of OVAL was displayed at the recent SANS Network Security 2002 conference and received an enthusiastic response from the technical audience in attendance.

The OVAL effort addresses the problem of how security assessment tools check for software vulnerabilities in different ways. If a computer is compared to a building and a vulnerability a way to get into the building, while one tool checks for doors and declares every door it finds a vulnerability, another tool checks to see whether the door is open or closed before declaring it a vulnerability, and yet another tool looks for large window as well as doors. These differences make it difficult to determine if any particular vulnerability is truly present.

OVAL builds upon Common Vulnerabilities and Exposures (CVE), a dictionary of standardized names and descriptions for publicly known information security vulnerabilities and exposures, developed by MITRE in cooperation with the international security community. The OVAL effort was initiated by MITRE, and involves representatives from a broad spectrum of industry, academia, and government organizations, including operating system and security tool vendors. Windows NT 4.0, Windows 2000, and Solaris 7 and 8, are OVAL's initial supported platforms. Red Hat Linux is supported in draft form.

"Rather than requiring any specific implementations for vulnerability assessment, OVAL provides a consistent, reliable, and common language for security experts to discuss the technical details of how to check for vulnerabilities on local computers," said Peter S. Tasker, executive director of MITRE's security and information operations division. "The end results of the discussions are collaboratively developed queries, which are an application of the OVAL language and perform the checks."

Queries are written in Structured Query Language (SQL) and can be reviewed individually by hand or incorporated into security tools. Each OVAL query is based on one or more CVE entries, and uses a community-developed schema. The query development process involves the submission of draft OVAL queries to a public forum that includes system administrators, software vendors, and security analysts for review, debate, and refinement. The resulting vulnerability content, in the form of approved OVAL queries for the supported platforms, is freely available over the Internet, and maintained by MITRE on the OVAL Web site (http://oval.mitre.org).

"OVAL solves the consistency problem," said Matthew N. Wojcik, MITRE senior information security engineer. "The queries provide a baseline for performing vulnerability assessments, and each query reflects the combined expertise of the broadest possible collection of security and system administration professionals. The widespread availability of OVAL queries will provide the means for standardized vulnerability assessment and result in consistent and reproducible information assurance metrics from systems."

"We're excited about OVAL's downstream potential," said Tasker. "This new effort will lead to enhanced vulnerability assessment tools and further innovations in information security."

About the MITRE Corporation

The MITRE Corporation (www.mitre.org) is a not-for-profit company that provides systems engineering, research and development, and information technology support to the government. Chartered to work in the public interest, MITRE operates federally funded research and development centers for the Department of Defense, the Federal Aviation Administration, and the Internal Revenue Service, with principal locations in Bedford, Massachusetts, and McLean, Virginia.

March 2002

FOR IMMEDIATE RELEASE

MITRE's CVE Lexicon of Information Security Vulnerabilities Surpasses 2,000 Entries

Bedford, MA, March 28, 2002 – The MITRE Corporation today announced that its Common Vulnerabilities and Exposures (CVE) dictionary has recorded more than 2,000 entries identifying specific computer vulnerabilities and exposures.

An international security community initiative, CVE (http://cve.mitre.org) is the first lexicon that provides standardized names and descriptions for publicly known information security vulnerabilities and exposures. CVE's common names make it easier to share data across separate network security databases and tools that are CVE-compatible. CVE also provides a baseline for evaluating the coverage of an organization's security tools.

The 2,000+ entries are a direct result of the work of the CVE Editorial Board, which over the last three years has increased to 49 organizations from industry, government, and academia around the world.

"This is an excellent example of the ongoing momentum of the CVE Initiative," said MITRE's CVE Project Leader Margie Zuk. "When we started in 1999 there were 321 official entries on the list and now there are 2,032, with an additional 1,994 candidate entries now being reviewed. This new milestone, along with growth in Editorial Board membership, strong increases in the numbers of organizations declaring their products and services CVE-compatible, and growing international participation, shows how fully the information security community has embraced the CVE Initiative."

Zuk added that CVE entries are included in the SANS/FBI "Twenty Most Critical Internet Security Vulnerabilities" consensus list, helping system administrators who use CVE-compatible products and services make their networks more secure.

The CVE Initiative also experienced extraordinary growth in the number of organizations committing to make their security products and services CVE-compatible. In total, 49 organizations from industry, government, and academia worldwide have declared that 75 network security products or services are or will be CVE-compatible. These organizations include BindView, the CERIAS Center at Purdue University, Cisco Systems, Harris, Internet Security Systems (ISS), the (USA) National Institute of Standards and Technology, Network Associates, SecurityFocus, and Symantec, among many others.

International participation in the initiative has also increased significantly. Seven members of the CVE Editorial Board are from outside the U.S., and 14 international organizations from seven countries around the world have committed to making their network security product and services CVE-compatible.

The number of vendors that have included CVE candidate numbers in their security advisories has increased to 21, and more than 300 candidates have appeared in vulnerability advisories to date. Including candidate numbers in advisories ensures that the community benefits by having CVE names as soon as the problem is announced. Organizations including candidate numbers on a regular basis are CERT/CC, ISS, Microsoft, and Red Hat.

"This ongoing, across-the-board growth truly exemplifies the important part CVE is playing in the global security community," concluded Zuk. "This can only improve even further as more vendors around the world and their customers embrace CVE compatibility in securing the enterprise."

About the MITRE Corporation

MITRE (www.mitre.org) is a not-for-profit company that provides systems engineering, research and development, and information technology support to the government. Chartered to work in the public interest, it operates federally funded research and development centers for the Department of Defense, the Federal Aviation Administration, and the Internal Revenue Service, with principal locations in Bedford, Massachusetts, and McLean, Virginia.

October 2000

FOR IMMEDIATE RELEASE

New Milestone for MITRE's Information Security Dictionary

More than 1,000 Entries now recorded

Bedford, MA, October 16, 2000 -- The MITRE Corporation has announced a new milestone in the Common Vulnerabilities and Exposures (CVE) dictionary, the first lexicon that provides standardized names and descriptions for publicly known information security vulnerabilities and exposures. CVE makes it easier for the information security community to share data across separate vulnerability databases and security tools.

As of today, the CVE dictionary has recorded more than 1,000 entries that identify specific computer vulnerabilities and exposures. "This is especially significant when you consider that CVE's size has nearly tripled in the past 12 months," said MITRE Lead Information Security Engineer Steve Christey, "and that doesn't include an additional 700 candidate entries that are now being reviewed. It never would have been possible without the active participation of so many leading organizations in the information security community."

Christey also serves as moderator of the CVE Editorial Board, which consists of a worldwide consortium of 30 commercial, academic and government organizations, including Microsoft, IBM, Ernst & Young, Sun Microsystems, Cisco Systems, Internet Security Systems, Network Associates, the CERIAS Center at Purdue University, the CERT Coordination Center and the SANS Institute.

In addition to this milestone, MITRE has upgraded its CVE Web site (cve.mitre.org) with new information and functionality. According to MITRE's CVE Project Manager Margie Zuk, "the site now allows users to sign up for e-mail notification of CVE updates and other timely CVE information. We've also added reference maps, which help users to quickly get CVE names using well-known security references."

"We've seen several other exciting developments in the past few months," added Christey. "CVE candidate names are starting to appear in announcements of new information security vulnerabilities, and companies continue to approach us about including CVE in their products. In fact, more than 25 organizations are now working towards making their own tools and databases CVE-compatible. The fact that the information security community has embraced the CVE Initiative will help make the Internet and other computer networks a far more secure environment for everyone."

About the MITRE Corporation
MITRE is a not-for-profit company that provides engineering services to the government. Chartered to work in the public interest, it operates Federally Funded Research and Development Centers for the DOD, the FAA and the IRS.

March 2000

FOR IMMEDIATE RELEASE

MITRE Employees Receive SANS Security Technology Leadership Awards

Bedford, MA, March 28, 2000 — In ceremonies last week at the SANS Joint Computer Security Conference in Orlando, FL, MITRE Corporation employees were presented with two SANS 2000 Security Technology Leadership Awards.

The first was given to MITRE’s Common Vulnerabilities and Exposures (CVE) team, consisting of Steve Christey, Margie Zuk, Pete Tasker, and Dave Mann (now with BindView), for "establishing, nurturing and sustaining the industry-wide cooperative CVE project." MITRE’s CVE initiative resulted in the world’s first lexicon that provides standardized names and descriptions for publicly known information security vulnerabilities and exposures. CVE makes it easier to share data across separate vulnerability databases and security tools.

MITRE’s Eric Kayden received an award as a member of the National Infrastructure Protection Center team, which was cited for its "leadership in the creation of forensics tools including software that isolates distributed denial of service attack tools."

"It means a lot to have been singled out by the SANS community," said Steve Christey who, along with David Mann, created CVE. "It couldn’t have been done without the full participation of the CVE Editorial Board and the vendor community. We continue to expand this board into other areas of the community, with our most recent additions being Microsoft and SUN Microsystems." MITRE established and leads the CVE Editorial Board, which includes representatives from 25 organizations in the private sector, the government and academia.

"I continue to be impressed by the steady increase in CVE acceptance," added MITRE's Margie Zuk. "A total of 21 producers of information security tools and databases have declared that they are making their products CVE-compatible. So far this month, the Editorial Board has agreed to add 53 new CVE entries, and MITRE has proposed an additional 120 candidates for review by the Board."

February 2000

FOR IMMEDIATE RELEASE

MITRE's Information Security Dictionary Reaches Important Milestones

Microsoft, Ernst & Young Join Editorial Board

Bedford, MA, February 3, 2000 -- The MITRE Corporation today announced new milestones in its unique Common Vulnerabilities and Exposures (CVE) dictionary, the first publicly available lexicon that provides standardized names and descriptions for publicly known information security vulnerabilities and exposures. CVE makes it easier to share data across separate vulnerability databases and security tools.

CVE's announcement last September was the result of a collaboration between MITRE, an independent, not-for profit company chartered to work for the government in the public interest, and 19 major security organizations that made up the CVE editorial board, including CERT Coordination Center, the SANS Institute, Network Associates, IBM Research, Cisco Systems and Internet Security Systems (ISS).

Since September, CVE (available at http://cve.mitre.org) has reached several important milestones:

- Seven new organizations are now represented on the CVE editorial board: Microsoft, Ernst & Young, Canadian CERT, GTE Internetworking, Hiverworld, ODS Networks, and Vista IT, bringing the total to 26.
- The number of CVE entries has reached 503, representing a 57% increase over the original entries.
- Nine members of the information security community have incorporated CVE into their products. Eight others have publicly declared their intentions to do so.
- Since its inception, CVE now has increased international reach and acceptance, including Canadian CERT, Alliance Qualitie Logiciel and CYRANO.
- CVE is now included in daily incident reports from the SANS Institute's Global Incident Analysis Center (GIAC). Further, the Computer Emergency Response Team Coordination Center (CERT) and MITRE have established a communication channel that will allow CVE names to be included in future CERT advisories. The GIAC reports and CERT advisories, both available as public services, allow readers to get current information about vulnerabilities that hackers might be exploiting. CVE's inclusion permits users to more easily correlate vulnerability information.
- Finally, proposed CVE entries (known as "candidates") have for the first time become publicly available on the latest version of MITRE's CVE web site, which was released today. These 535 candidates are being considered by the editorial board for possible inclusion in the CVE list.

"CVE's growth has exceeded even our own optimistic expectations," says editorial board chair Steve Christey, a MITRE senior software analyst. "The rate at which it's being adopted is a good indicator of how strongly the information security community feels about information-sharing. We continue to see new uses of CVE in different areas of information security."

September 1999

FOR IMMEDIATE RELEASE

MITRE and Top Security Organizations Launch First Public Dictionary of Computer Vulnerabilities to Boost Cyber-Defense

Dictionary to Enhance Information Sharing and Improve Security Tools

Bedford, MA, Sept. 29, 1999 - The MITRE Corporation today announced the new Common Vulnerabilities and Exposures (CVE) initiative, the first publicly available dictionary that provides standardized names and descriptions for more than 300 publicly known information security vulnerabilities and exposures. CVE is expected to boost cyber defenses by making it easier to share data across separate vulnerability databases and security tools. MITRE, an independent, not-for profit company working in the public interest, developed the CVE list in cooperation with 19 major security organizations that make up the CVE Editorial Board, including CERT Coordination Center, IBM Research, Cisco Systems and Internet Security Systems (ISS).

"In the past, each security tool and vulnerability database used its own names for vulnerabilities and exposures. Without a common language to correlate pieces of vulnerability-related information, it was difficult to manage the output from the security tools that we use," said Pete Tasker, Executive Director of Security and Information Operations at MITRE. "CVE will help us better serve our sponsors and protect our security perimeter by making it easier to share information."

In addition to facilitating data sharing among Intrusion Detection Systems (IDSs), assessment tools, vulnerability databases, researchers and incident response teams, CVE will provide a basis to achieve security tool interoperability and comparisons across vendor platforms and facilitate vulnerability research.

"The CVE naming standard developed by MITRE represents a significant leap forward for the information security industry and end user community," said Christopher Klaus, founder and chief technology officer of Internet Security Systems. "As a technology pioneer and leading provider of security management software and services, ISS is pleased to be a part of this important initiative as we move toward a standard that is crucial to the effective protection of every organization's critical digital assets."

The comparative research made possible by CVE is expected to lead to enhanced security tools and further innovations in information security.

"CVE is a scientific necessity," said Bill Fithen, senior analyst, Computer Emergency Response Team (CERT). "It will facilitate improved communication among information assurance professionals in many ways. We believe there will be many beneficiaries of the CVE: system and network administrators, IT managers, security product consumers, researchers, teachers, and students."

The CVE Editorial Board includes representatives from top security-related organizations from the private, academic and government sectors. Editorial board members include: AXENT Technologies, The Ballistic Missile Defense Organization, BindView Development, Bugtraq, CyberSafe, CERIAS/Purdue University, Harris Corp (STAT Operations), L-3 Network Security, Network Associates Inc. (NAI), Network Flight Recorder (NFR), NTBugtraq, SANS Institute, SecurityFocus.com, Silicon Defense and University of California - Davis.

MITRE plans to make CVE available to the public through a web site scheduled for release on Wednesday (cve.mitre.org). MITRE, an independent, not-for-profit company providing technical support to government in the public interest, is a center of excellence for information assurance.

For the latest News, Blogs, Podcasts, and Press Releases, visit All News on the CVE website.