# 2015 News — Archive

**CVE Included in ITU's "Security in Telecommunications and Information Technology 2015"**

December 10, 2015

CVE is included in a September 2015 technical report entitled "Security in Telecommunications and Information Technology 2015" on the International Telecommunication Union (ITU) website. The main topic of the report is an "overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications."

CVE is mentioned in "Chapter 11 - Cybersecurity and incident response," as the main topic of section "11.1.2 Exchange of vulnerability information," as follows: "Recommendation ITU-T X.1520 on the common vulnerabilities and exposures (CVE) provides a structured means to exchange information on security vulnerabilities and exposures and provides a common identifier for publicly-known problems. This Recommendation defines the use of CVE to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this common identifier. This Recommendation is designed to allow vulnerability databases and other capabilities to be used together, and to facilitate the comparison of security tools and services. CVE contains only the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories. (It does not contain information such as risk, impact, fix information, or detailed technical information). The primary focus of CVE is to identify known vulnerabilities and exposures that are detected by security tools along with any new problems that are detected."

In addition, Common Vulnerability Scoring System (CVSS) is the main topic of section 11.1.3 Vulnerability scoring," and DHS's Common Weakness Enumeration (CWE™) is the main topic of section "11.1.4 Exchange of weakness information," Common Weakness Scoring System (CWSS™) is the main topic of section "11.1.5 Weakness scoring," and Common Attack Pattern Enumeration and Classification (CAPEC™) is the main topic of section "11.1.5 Exchange of attack pattern information," and Malware Attribute Enumeration and Characterization (MAEC™) is the main topic of section "11.1.7 Exchange of malware characteristics information."

**CVE Mentioned in Article about Apple's December Security Fixes for OS X and iOS on eWeek**

December 10, 2015

CVE is mentioned in a December 9, 2015 article entitled "Apple Updates OS X, iOS With Numerous Security Fixes" on eWeek. The main topic of the article is "security updates for [Apple's] desktop Mac OS X 10.11 and mobile iOS 9 operating systems … including networking, graphics and wireless operations."

The CVE IDs cited in this article include the following: CVE-2015-7110, CVE-2015-7078, CVE-2015-7106, CVE-2015-7077, CVE-2015-7112, CVE-2015-7068, CVE-2015-7083, CVE-2015-7084, CVE-2015-7047, CVE-2015-7112, CVE-2015-7068, CVE-2015-7094, CVE-2015-7073, CVE-2015-7015, CVE-2015-7037, and CVE-2015-7080.

In addition, Apple is a CVE Numbering Authority (CNA), assigning CVE IDs for Apple issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs to newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

**CVE Mentioned in Article about Microsoft's Patch Tuesday Fixes for December on Threatpost**

December 10, 2015

CVE is mentioned in a December 8, 2015 article entitled "Microsoft Patches 71 Flaws, Two Under Attack; Warns of Leaked XBox Live Cert" on Threatpost. The main topic of the article are the fixes included in Microsoft's Patch Tuesday for December.

CVE is first mentioned in the article with regard to the two vulnerabilities currently under attack, as follows: "… Microsoft released a dozen bulletins today, eight of which it rates as Critical—in particular, the two vulnerabilities currently under attack. The Office vulnerability, CVE-2015-6124, is one of six patched in MS15-131, and is described only as a memory-corruption vulnerability, one of five such flaws patched in the bulletin." "The other vulnerability under attack, CVE-2015-6175, is a kernel memory elevation of privilege in Windows; it's one of four such flaws patched in MS15-135. An attacker would need local access and privileges to a vulnerable Windows client or server, and a successful exploit would allow an attacker to install malware or manipulate data on the compromised computer."

In addition, Microsoft is a CVE Numbering Authority (CNA), assigning CVE IDs for Microsoft issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs to newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

Visit CVE-2015-6124 and CVE-2015-6175 to learn more about these issues.

**CVE Mentioned in Article about Two Critical JavaScript Vulnerabilities on InfoWorld**

December 10, 2015

CVE is mentioned in a November 25, 2015 article entitled "Node.js discloses two critical security vulnerabilities" on InfoWorld, as follows: "A bulletin issued today by the Node.js Foundation, which has jurisdiction over the popular server-side JavaScript platform, covers "a high-impact denial-of-service vulnerability" and a "low-impact V8 out-of-bounds access vulnerability." V8 is the Google-developed JavaScript engine leveraged by Node.js. Officially, the DoS issue is labeled as CVE (Common Vulnerabilities and Exposures) 2015-8027, while the access problem is identified as CVE-2015-6764."

Visit CVE-2015-8027 and CVE-2015-6764 to learn more about these issues.

**CVE Mentioned in Article about Effect of Android's Stagefright Vulnerability in Q3-2015 on DataQuest**

December 10, 2015

CVE is mentioned in a November 24, 2015 article entitled "95% of Android devices were affected in Q3, 2015, reports Trend Micro" on DataQuest.

CVE is mentioned as follows: "The Stagefright vulnerability affected nearly 95% of all Android devices out there. In total, five different vulnerabilities in media processing in Android were attacked this quarter. Stagefright (CVE-2015-3824), which allows attackers to install malware on affected devices by distributing malicious Multimedia Messaging Service (MMS) messages, reportedly put 94.1% of Android devices (as of this July) at risk. We also found a bug that could render Android phones silent and unable to make calls or send text messages. Reports said more than 50% of Android devices (as of this July) were vulnerable to this flaw. Another critical Mediaserver vulnerability (CVE-2015-3823), which could cause devices to endlessly reboot and allow attackers to remotely run arbitrary code, was also found. At that time, 89% of Android devices were susceptible to exploitation. CVE-2015-3842, which could allow remote code execution in Mediaserver's AudioEffect component, also figured in the landscape this August 26."

Visit CVE-2015-3823, CVE-2015-3824, CVE-2015-3825, and CVE-2015-3842 to learn more about these issues.

**CVE Mentioned in Press Release about Container Security for Enterprise Computing**

December 10, 2015

CVE is mentioned in a November 10, 2015 press release entitled "Twistlock Strengthens Container Security for Enterprise Computing" on MarketWired. The main topic of the press release is a product release announcement by Twistlock for its Twistlock Container Security Suite.

CVE is mentioned in the release in a quote by Wix System Team Manager Gregory Man, who states: "Security is a top priority for Wix, and Twistlock has made it easier for us to protect our customers as we adopt new technologies like containers. The integration with CVE databases has been particularly valuable in identifying and fixing vulnerabilities within containers, and the hardening policies help us enforce the same security standards throughout the application lifecycle."

**CVE Mentioned in Article about Multiple Network Time Protocol (NTP) Vulnerabilities on eWeek**

November 24, 2015

CVE is mentioned in an October 26, 2015 article entitled "Cisco Exposes, Helps Patch Multiple NTP Vulnerabilities" on eWeek. The main topic of the article is that "Cisco security researchers help to discover multiple vulnerabilities in the Network Time Protocol [NTP]," a "core element of the Internet infrastructure, quite literally helping the technology world as we know it stay on time."

The CVE IDs cited in this article include eight security vulnerabilities in NTP: CVE-2015-7848, CVE-2015-7849, CVE-2015-7850, CVE-2015-7851, CVE-2015-7852, CVE-2015-7853, CVE-2015-7854, and CVE-2015-7871.

Cisco is a CVE Numbering Authority (CNA), assigning CVE IDs for Cisco issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

**CVE Mentioned in Article about a Critical Vulnerability in Xen Cloud Hosting Platform on Ars Technica**

November 24, 2015

CVE is mentioned in an October 29, 2015 article entitled "Xen patches 7-year-old bug that shattered hypervisor security" on Ars Technica. The main topic of the article is that a "Critical vulnerability allowed some guests to access underlying operating system" in some cloud computing services.

The author states: "For seven years, Xen virtualization software used by Amazon Web Services and other cloud computing providers has contained a vulnerability that allowed attackers to break out of their confined accounts and access extremely sensitive parts of the underlying operating system. The bug, which some researchers say is probably the worst ever to hit the open source project, was finally made public Thursday along with a patch."

CVE is mentioned as follows: "As a result of the bug, "malicious PV guest administrators can escalate privilege so as to control the whole system," Xen Project managers wrote in an advisory. The managers were referring to an approach known as paravirtualization, which allows multiple lower-privileged users to run highly isolated computing instances on the same piece of hardware. By allowing guests to break out of those confines, CVE-2015-7835, as the vulnerability is indexed, compromised a core tenet of virtualization."

Visit CVE-2015-7835 to learn more about this issue.

**After 16+ Years, CVE Co-Founder Steve Christey Coley Departs the CVE Project**

November 12, 2015


Steve Christey Coley at the CVE/CWE booth at *RSA 2013*

Steve Christey Coley, the co-founder of CVE who served as the project's technical lead, CVE Editorial Board moderator, and Editor of the CVE List since the project was launched publicly in 1999, resigned from the CVE project on October 26th.

Steve, who will be staying at MITRE, will now focus primarily on being the technical lead for the Common Weakness Enumeration (CWE™) project and addressing the vulnerability management needs of the healthcare industry, while also keeping the CVE concept in mind. As Steve mentions in his departure message to the CVE Editorial Board: "My current work in CWE and healthcare … is likely to expand into other industry verticals with emerging cybersecurity challenges. I also plan to investigate what "CVE" would mean in other industry verticals and emerging technical domains, and/or in other global regions. I'll even be drawing from my experience in my old AI days of the early 90's."

Steve also intends to stay very involved in the vulnerability world by continuing to "advocate for and support the development of the next generation of vulnerability researchers; to build that ever-elusive theoretical framework for precisely understanding vulnerabilities, weaknesses, and their root causes; and to help "InfoSec" mature as an industry, including embracing people with non-traditional or non-technical roles that are critical to the industry's maturation. I will also seek to encourage diversity (in all its forms) within this industry; I believe that InfoSec has great potential for positive change, because we've all been outsiders in one way or another."

**Origin Story**

Steve Christey Coley with former CVE Project Lead Pete Tasker and CVE Editorial Board Emeritus member Adam Shostack at CVE's 10-year anniversary celebration in 2010

It all started back in 1998 when a MITRE Lead Information Security Engineer named Steve Christey Coley was trying to choose a commercial vulnerability assessment tool to help protect MITRE's own networks, and was dealing first-hand with the problem of multiple vulnerabilities that were the same issue but had different names, were described in different ways, and that tested at different levels of abstraction. In an attempt to decipher this confusion, Steve did a labor-intensive mapping across the commercial tools that he was considering at that time and learned that there were many discrepancies in coverage claims; some tools provided less coverage than claimed, while others provided more.

At the same time, MITRE's David Mann was trying to develop a database of system characteristics for the corporation that could be used to answer questions about how vulnerable MITRE was to problems described by security advisories.

Steve and Dave combined their efforts and developed a proposal for a simple common naming scheme that could be used by the community to correlate vulnerability information. They presented their approach, "Towards a Common Enumeration of Vulnerabilities," at a Purdue University vulnerability database workshop in January of 1999. That approach eventually grew into the CVE we know today 16+ years later.

**A Special Thank You to the Team and Community from Steve**

Steve Christey Coley having fun with co-founders Dave Mann and Margie Zuk in 1999

In his departure message, Steve emphasized that CVE has always very much been a collaborative effort, and gave special thanks to fellow CVE co-founder David Mann for his "passion, principles, and far-forward, out-of-the-box thinking" and to Margie Zuk, "the third member of the original CVE triad, whose contributions to CVE have gone woefully unrecognized; whose unique combination of unmitigated optimism, realistic pessimism, and patience kept the project moving forward through some tough times … and whose original admonition to "keep the faith" back in spring 1999 has served me countless ways over the years."

Steve also thanked the entire CVE community: "On a broader scale, my humblest thanks and appreciation go to the hundreds of people in the entire CVE community, with whom I've had the pleasure of working: the ever-changing members of the CVE content team, each of whom has brought their own perspective and skills, and left their own mark; numerous MITRE employees, from senior management who supported the idea and took a risk in CVE's founding years, to the specialists from other disciplines who contributed their expertise to improve our processes, to the admin support who helped everything run smoothly; the members of the CVE Editorial Board, who taught me to think more comprehensively about the many different perspectives surrounding vulnerability management, and whose endorsement of CVE gave it the legitimacy to effect positive change in the industry; independent and hobbyist researchers, whose contributions to the industry's body of knowledge and my own intellectual growth have been consistently underestimated; and countless other people I've talked to by email, at conferences, or on social media."

### Wishing Steve Well

Current CVE Project Lead Steve Boyle posted a "Very Special Thank You to Steve Christey Coley" message to the CVE Editorial Board email discussion list on October 28th, saying: "Steve has been a mentor and teacher to many people, both inside and outside of MITRE. He is, and has been for many years, a highly engaged, respected and respectful member of the community. We extend our deepest thanks to Steve and wish him all the best in his new endeavors. Congratulations, people who are about to begin working with Steve, you do not yet know how lucky you are."

We echo that sentiment here: Thank you Steve for all you have done and best of luck in your new endeavors!

### New CVE Editorial Board Member for Red Hat

November 3, 2015

Kurt Seifried of Red Hat, Inc. has joined the CVE Editorial Board.

Read the full announcement and welcome message in the CVE Editorial Board email discussion list archive.

### CVE Mentioned in Article about Joomla Vulnerabilities Affecting Millions of Websites on Ars Technica

October 27, 2015

CVE is mentioned in an October 23, 2015 article entitled "Joomla bug puts millions of websites at risk of remote takeover hacks" on Ars Technica. The main topic of the article is that "Millions of websites used in e-commerce and other sensitive industries are vulnerable to remote take-over hacks made possible by a critical vulnerability that has affected the Joomla content management system for almost two years."

The author states: "The SQL-injection vulnerability was patched by Joomla on Thursday with the release of version 3.4.5. The vulnerability, which allows attackers to execute malicious code on servers running Joomla, was first introduced in version 3.2 released in early November 2013. Joomla is used by an estimated 2.8 million websites." CVE is mentioned as follows: "The vulnerability, and two closely related security flaws, have been cataloged as CVE-2015-7297, CVE-2015-7857, and CVE-2015-7858."

Visit CVE-2015-7297, CVE-2015-7857, and CVE-2015-7858 to learn more about these issues.

### CVE Identifier "CVE-2015-7645" Cited in Numerous Security Advisories and News Media References about a Zero-Day Adobe Flash Vulnerability

October 27, 2015

"CVE-2015-7645" is cited in numerous major advisories, posts, and news media references related to the recent zero-day Adobe Flash vulnerability, including the following examples:

http://neurogadget.com/2015/10/26/adobe-flash-player-19-0-0-226-patched-a-vulnerability-is-it-still-worth-it/18430

http://arstechnica.com/security/2015/10/new-zero-day-exploit-hits-fully-patched-adobe-flash/

http://bgr.com/2015/10/15/adobe-flash-player-security-vulnerability-warning/

http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/

http://venturebeat.com/2015/10/14/adobe-confirms-new-critical-flash-vulnerability-is-being-exploited-in-targeted-attacks-promises-patch-next-week/

https://threatpost.com/emergency-adobe-flash-zero-day-patch-arrives-ahead-of-schedule/115073/

http://www.welivesecurity.com/2015/10/15/adobe-flash-zero-day/

http://www.ibtimes.co.uk/adobe-admits-critical-vulnerability-flash-player-19-0-0-207-earlier-versions-1524229

http://bgr.com/2015/10/16/adobe-flash-player-security-vulnerability-patch-download/

http://www.scmagazine.com/adobe-issues-advisory-for-flash-vulnerability-targeting-government-agencies/article/445181/

http://www.ubergizmo.com/2015/10/adobe-confirms-critical-vulnerability-in-some-flash-versions/

http://www.slashgear.com/adobe-flash-has-a-new-critical-vulnerability-on-all-platforms-15409916/

Other news articles may be found by searching on "CVE-2015-7645" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7645 includes a list of advisories used as references.

### CVE Included in Cisco's Recently Updated Vulnerability Disclosure Process

October 13, 2015

CVE is included in Cisco Systems, Inc.'s refined security disclosure process, as described in an October 5, 2015 blog post entitled "Streamlining the Response to Security Vulnerabilities" on its security blog. CVE is mentioned as benefit 4 of 5 as what's new in the process, as follows: "Every vulnerability assigned a Common Vulnerability and Exposures (CVE). Aids in identification and search."

Release of the updated policy also resulted in CVE being cited in numerous major news media references and posts, including the following examples:

http://www.eweek.com/security/cisco-redefines-how-it-manages-communicates-security-issues.html

http://www.theregister.co.uk/2015/10/06/cisco_reforms_its_security_disclosure_process/

http://www.scmagazineuk.com/cisco-develops-new-and-improved-security-disclosure-process/article/443429/

http://www.programmableweb.com/news/%E2%80%8Bcisco-to-use-api-to-distribute-detailed-security-vulnerability-advisories/2015/10/08

http://blogs.cisco.com/security/psirt-u

https://dutchitchannel.nl/537988/cisco-vernieuwt-beleid-rond-vulnerabilities-in-producten.html

Cisco is a CVE Numbering Authority (CNA), assigning CVE IDs for Cisco issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

**Two CVE Identifiers Cited in Numerous Security Advisories and News Media References about the Android "Stagefright 2.0" Vulnerability**

October 13, 2015

Two CVE Identifiers — CVE-2015-6602 and CVE-2015-3876 – are cited in numerous major advisories, posts, and news media references related to the recent Android "Stagefright 2.0" vulnerability, including the following examples:

http://www.infosecurity-magazine.com/news/google-releases-patches-for/

http://www.eweek.com/security/google-patches-stagefright-2-android-vulnerability.html

http://www.theregister.co.uk/2015/10/06/stagefright_fixes_pushed/

http://www.linuxinsider.com/story/82570.html

http://www.heraldcurrent.com/stagefright-the-dreaded-android-vulnerability-is-back/12670/

https://www.whatech.com/mobile-apps/press-release/98548-kagiso-interactive-best-developers-for-mobile-apps

http://news.softpedia.com/news/google-releases-stagefright-2-0-fix-493799.shtml

http://www.theoracleobserver.com/new-stagefright-bug-lets-hackers-infect-androids-through-multimedia-files/5902/

http://www.darkreading.com/vulnerabilities---threats/stagefright-20-vuln-affects-nearly-all-android-devices-/d/d-id/1322446

http://www.itnews.com.au/news/new-stagefright-bug-menaces-over-a-billion-android-devices-409972

https://threatpost.com/stagefright-2-0-vulnerabilities-affect-1-billion-android-devices/114863/

http://fortune.com/2015/10/01/stagefright-android-vulnerability-song/

http://www.zaikei.co.jp/article/20151004/272192.html

http://punto-informatico.it/4274025/PI/News/stagefright-20-torna-paura-android.aspx

http://www.computerbase.de/2015-10/android-google-veroeffentlicht-patch-fuer-stagefright-2.0/

http://branchez-vous.com/2015/10/01/stagefright-2-0-les-appareils-android-nouveau-vulnerables/

Other news articles may be found by searching on "CVE-2015-6602" and "CVE-2015-3876" using your preferred search engine. Also, the CVE Identifier pages https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6602 and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3876 include lists of advisories used as references.

**Upcoming Changes to CVE**

October 1, 2015

We would like to take this opportunity to notify the CVE Editorial Board and the community of changes that are coming for CVE.

We recognize that there is deep frustration with some aspects of CVE, and that there are areas in need of updating after 16 years of continuous operation. We have been working on a number of things to improve our internal processes and workflow and will start to make visible changes to CVE in the coming weeks and months.

The operation and use of CVE has significantly evolved in the last 16 years. While CVE has served the community very well, its current operating model is proving to be unable to keep up with the breadth and volume of CVE requests and subsequent production of final CVE entries.

Our intent is to be heavily engaged with the CVE community and users, now and even more so in the future, and to be completely transparent about what we are doing and why. If you believe at any time that we are not meeting those goals, we respectfully request your engagement and feedback telling us where we are falling short so that we can better understand the needs and requirements of the community.

CVE Editorial Board

The CVE Editorial Board was created to define and shape CVE, even before CVE first went public. The Board's operating model and framework have evolved significantly in the years since as the community and requirements have evolved. Today, the community is more dynamic than it was even just a few years ago, and the Board model is in need of a refresh. To that end, Julie Connolly, a new member of the MITRE CVE Team, is taking on the role of liaison from MITRE to the Board.

Julie will be putting out an email that will outline what we believe are the objectives for a Board refresh, including responsibilities, membership, and a number of other aspects that have been discussed. Julie will provide more details in her email, and we hope the Board will be very engaged as we seek your suggestions, feedback, and comments to help us refresh, shape, and formalize a number of aspects of the CVE Editorial Board and its operation.

CVE Numbering Authorities (CNAs)

The CVE CNAs are another aspect of CVE that was instantiated years ago, and have proven valuable to the operation of CVE. As with the Board, the operation of and requirements on CNAs have evolved significantly and need to be updated. In particular, as the volume of requests for CVE IDs continues to increase, the need for, definition of the role, and the successful operation of CNAs becomes even more critical to CVE and the community.

Tiffany Bergeron of the MITRE CVE Team is taking the lead for CNAs, and will be emailing this list to describe requirements and objectives for CNAs and to solicit suggestions, feedback and comments from the Board.

Tiffany will be engaging with the Board, and will email to describe the objectives and plans for updating multiple aspects of the CNA relationship and functioning. Our aim is to improve both sides of the operation and reliability of CNAs, to have CNAs evolve to take on a larger role in the creation of CVEs, and to ultimately expand the number of CNAs.

CVE Assignment (CVE ID Requests)

No single aspect of CVE has been more problematic or engendered more frustration for both the community and for CVE than the process of requesting and assigning CVE IDs for newly discovered vulnerabilities. We will begin to implement changes in the next few days that will result in reasonable response times and process improvements, and to put in place new feedback mechanisms for requesters. We will be providing documented guidelines for requesting CVE IDs, including required elements and criteria. Because of the increasing volume of requests, we are planning to push more responsibility for well-constructed and informational requests back onto the requesters, rather than provide individual, educational responses as we sometimes have in the past. We will, of course, always be available to help researchers and disclosers understand what goes into a "good" CVE request, and we will be providing documentation to help both first-time and experienced requesters.

Steve Boyle is taking responsibility for this area and will be following up with changes and plans. We are actively seeking additional comments, suggestions, and feedback from the community to help us shape the process, feedback, and utility of CVE ID requests.

Moving Forward

MITRE has never, and will never, presume that "we know best" for CVE and its use within the community. The original operating principle of being guided by the Board remains as important as it ever has been in the history of CVE. For our part, we will be working to actively demonstrate more engagement and transparency with the Board and with the community.

If you are a Board member, please provide any responses to the CVE Editorial Board Email Discussion List. For others, please send your feedback to cve@mitre.org.

Thank you for your advice and engagement to date. We look forward to your comments and input as we move forward with the evolution of CVE.

Steve Boyle MITRE

CVE Project Leader

NOTE: The information above was previously posted to the CVE Editorial Board Email Discussion List on September 24, 2015.

**1 Product from Hillstone Networks Now Registered as Officially "CVE-Compatible"**

October 1, 2015

One additional information security product has achieved the final stage of MITRE's formal CVE Compatibility Process and is now officially "CVE-Compatible." The product is now eligible to use the , and a completed and reviewed "CVE Compatibility Requirements Evaluation" questionnaire is posted for the product as part of the organization's listing on the CVE-Compatible Products and Services page on the CVE Web site. A total of 148 products to-date have been recognized as officially compatible.

The following product is now registered as officially "CVE-Compatible":

Hillstone Networks - Next Generation Firewall

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 and services 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.

**CVE Mentioned in Article about Vulnerabilities Fixed by Apple's iOS 9 on eWeek**

September 24, 2015

CVE is mentioned throughout a September 17, 2015 article entitled "Apple's iOS 9 Addresses Long List of Vulnerabilities" on eWeek. The main topic of the article is that "In addition to many new features, Apple's iOS 9 addresses a long list of security vulnerabilities."

The CVE IDs cited in this article include: CVE-2015-5916, which "erroneously enables transaction log functionality on some configurations" of Apple Pay; CVE-2015-5850, which "could have enabled an attacker to reset a passcode with an iOS backup"; CVE-2015-5832, "a vulnerability in which AppleID credentials remained persistent in iOS even after a user signed out"; CVE-2015-5837, which "could have enabled a malicious enterprise application to install extensions, even if the application is not yet trusted by the enterprise"; CVE-2015-5858, "a Web address parsing flaw in handling HSTS (HTTP Strict Transport Security)" [in CFNetwork]; and CVE-2015-5860, "another CFNetwork flaw in HSTS handling that affects the Safari Web browser … [through which] … an attacker could have potentially tracked users in Safari private browsing mode".

In addition, Apple is a CVE Numbering Authority (CNA), assigning CVE IDs for Apple issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs to newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

Visit CVE-2015-5916, CVE-2015-5850, CVE-2015-5832, CVE-2015-5837, CVE-2015-5858, and CVE-2015-5860 to learn more about these issues.

**CVE IDs Used throughout Qualys' July 2015 "Top 10 Vulnerabilities" List**

September 24, 2015

CVE IDs are used throughout Qualys, Inc.'s July 2015 "Top 10 Vulnerabilities" lists to uniquely identify the vulnerabilities referenced on its top 10 external and top 10 internal vulnerabilities lists. The two lists are "dynamic lists of the most prevalent and critical security vulnerabilities in the real world."

According to the Qualys website, the two lists are "Based on the Laws of Vulnerabilities, this information is computed anonymously from over 1 billion IP audits per year. The Top 10 External Vulnerabilities are the most prevalent and critical vulnerabilities which have been identified on Internet facing systems. The Top 10 Internal Vulnerabilities show this information for systems and networks inside the firewall."

Review the July 2015 release of Qualys' Top 10 External Vulnerabilities and Top 10 Internal Vulnerabilities lists at: https://www.qualys.com/research/top10/.

**CVE Mentioned in Article about a Microsoft Word Vulnerability Being Exploited via Email on Naked Security**

September 15, 2015

CVE is mentioned in a September 8, 2015 article entitled "Anatomy of a malicious email: Crooks exploiting recent Word hole" on Naked Security.

The author states: "SophosLabs has drawn our attention to a new wave of malware attacks using a recent security bug in Microsoft Word. The bug, known as CVE-2015-1641, was patched by Microsoft back in April 2015 in security bulletin MS15-033. The vulnerability was declared to be

"publicly disclosed," meaning that its use wasn't limited only to the sort of crooks who hang out in underground exploit forums. Of course, turning a potential Remote Code Execution (RCE) vulnerability into a reliably-working exploit isn't always as easy as it sounds, but that has happened here." The article also includes a detailed analysis of how the attacks occur.

Visit CVE-2015-1641 to learn more about this issue.

**CVE Mentioned in Article about Vulnerabilities in HP PCs, Laptops, and Tablets on TechWorm**

September 15, 2015

CVE is mentioned in a September 13, 2015 article entitled "Hackers can remotely exploit bug in HP PCs, Laptops and Tablets" on TechWorm. The main topic of the article is that "The HP PCs/Laptops and Notebooks which have HP lt4112 LTE/HSPA+ Gobi 4G Module onboard, have been found to have critical vulnerabilities which can be exploited by potential hackers to remotely execute arbitrary code."

CVE is mentioned when the author states: "The vulnerability listed under CVE-2015-5367 allows a potential attacker to exploit this flaw to obtain the root permission, access the system by connecting the serial port, and view or modify configuration." CVE is mentioned again when the author states: "While the CVE-2015-5368 allows an attacker to tamper with the upgrade package, leading to an upgrade failure or the upgrade of an incorrect package. As a result, services may become unavailable."

Visit CVE-2015-5367 and CVE-2015-5368 to learn more about these issues.

**CVE Mentioned in Article about Seagate Patching 3 Backdoor Vulnerabilities on eWeek**

September 15, 2015

CVE is mentioned throughout a September 8, 2015 article entitled "Seagate Patches for 3 Backdoor Security Vulnerabilities" on eWeek. CVE is first mentioned when the author states: "Seagate is advising users of its Wireless Mobile Storage and LaCie FUEL hard drives to update the embedded firmware to patch for multiple known vulnerabilities that could potentially enable a remote attacker to gain unauthorized access to a user's information. In new firmware updates, Seagate is patching for three vulnerabilities (CVE-2015-2874, CVE-2015-2875 and CVE-2015-2876)."

CVE is mentioned a second time, when the author states: "Among the flaws that Seagate is patching is a hard-coded administrative credentials issue (CVE-2015-2874). The hard-coded credentials included a default administrative account with the username and password of "root." … the impact of the CVE-2015-2874 vulnerability is that an attacker could take control of a user's hard drive and also potentially use the device as a base from which to launch other attacks."

CVE is mentioned a third time, when the author states: "Another patched issue (CVE-2015-2875) is a direct-request, forced-browsing flaw. Under a default configuration, Seagate wireless hard drives provide an unrestricted file download capability to anonymous attackers with wireless access to the device," CERT warns … " CVE is mentioned a fourth time, when the author states: "The third issue that Seagate is patching, CVE-2015-2876, is an "unrestricted upload of file with dangerous type" flaw. The issue is that the unpatched firmeware allows access to a section of the hard drive that is intended to be used for file-sharing."

Visit CVE-2015-2874, CVE-2015-2875, and CVE-2015-2876 to learn more about these issues.

**CVE Mentioned in Article about Vulnerabilities in Baby Monitors on SC Magazine**

September 15, 2015

CVE is mentioned in a September 2, 2015 article entitled "Baby monitor vulnerabilities bring IoT security issues into sharp focus" on SC Magazine. The main topic of the article is that "In research that should strike fear in the heart of any new parent—and those professionals concerned about the security implications of the Internet of Things—a security pro at Rapid7 found vulnerabilities in commonplace retail video baby monitors that not only offer prying eyes a look into a family's most intimate moments, but could also "provide a path to compromise of the larger, nominally external, organizational network."

CVE is mentioned when the author states: "Rapid7 disclosed its findings "to the individual vendors, to CERT, and to the public, in accordance with Rapid7's Disclosure Policy1. CVE-2015-2880 through CVE-2015-2889 (inclusive) were assigned by CERT," the report said. "Typically, these newly disclosed vulnerabilities are only effectively mitigated by disabling the device and applying a firmware update when one becomes available, or with updates to centralized vendor cloud services."

Visit CVE-2015-2880, CVE-2015-2881, CVE-2015-2882, CVE-2015-2883, CVE-2015-2884, CVE-2015-2885, CVE-2015-2886, CVE-2015-2887, CVE-2015-2888, and CVE-2015-2889 to learn more about these issues.

**CVE Mentioned in Article about a Severe iOS Sandbox Vulnerability on ZDNet**

August 25, 2015

CVE is mentioned in an August 21, 2015 article entitled "Enterprise placed at risk by iOS sandbox vulnerability" on ZDNet. The author states: "A vulnerability which exploited iOS mobile device management (MDM) solutions was able to expose enterprise credentials used by apps and for corporate server access has been patched. Last week, the iPad and iPhone maker fixed the 'Quicksand' flaw, CVE-2015-5749, which utilizes a third-party sandbox flaw to harvest credentials used by enterprise mobile applications. According to mobile security firm Appthority, the previously unknown flaw impacts on MDM clients as well as any applications which are distributed through an MDM's Managed App Configuration settings, used to configure and store settings and data."

Visit CVE-2015-5749 to learn more about this issue.

**CVE Mentioned in Article about Multiple Android Vulnerabilities on Dark Reading**

August 25, 2015

CVE is mentioned in an August 20, 2015 article entitled "The Month Of Android Vulnerabilities Rolls On" on Dark Reading. The main topic of the article is that "Starting with the critical vulnerability in the Stagefright multimedia engine -- released at the end of July and detailed at Black Hat in early August -- Android security has received a relentless pummeling for weeks. Several of the new vulnerabilities discovered also leverage weaknesses in Android's handling of multimedia, and none of them will be easily repaired by a mere patch."

CVE is mentioned with regard to the first of six vulnerabilities discussed in the article, when the author states: "This week, Trend Micro researchers released details about a Stagefright-like vulnerability (CVE-2015-3842) in AudioEffect, a component of MediaServer, that affects Android versions 2.3 through 5.1.1. The bug could enable arbitrary code execution and give the attacker the same permissions as MediaServer, which has access to the device's camera, photos, and videos." CVE is mentioned a second time, when the author states: "Another vulnerability in MediaServer (CVE-2015-3823) affects Android versions 4.0.1 to 5.1.1 and enabled denials of service, sending Android devices into a cycle of endless reboots."

Visit CVE-2015-3842 and CVE-2015-3823 to learn more about these issues.

**CVE Mentioned in Article about a Zero-Day Internet Explorer Vulnerability on Computing**

August 25, 2015

CVE is mentioned in an August 19, 2015 article entitled "Microsoft rushes out emergency patch to fix zero-day Internet Explorer security flaw" on Computing.

The author states: "Microsoft has rushed out an emergency, out-of-band patch to fix a "critical" zero-day security flaw in the Internet Explorer web browser - one that, it warns, hackers may already be exploiting. The vulnerability, CVE-2015-2502, enables remote code execution, according to Microsoft bulletin MS15-093. "The vulnerability could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user," according to the Bulletin."

Visit CVE-2015-2502 to learn more about this issue.

**CVE Mentioned in Article about a Severe DNS Vulnerability on The Next Web**

August 25, 2015

CVE is mentioned in an August 3, 2015 article entitled "A huge DNS exploit could take down chunks of the internet" on The Next Web. The author states: "… CVE-2015-5477 details an exploit that allows a remote, unauthenticated attacker to crash DNS servers using BIND by sending a specially crafted command. There's no specific way to protect against the attack, other than installing the patch immediately. The attack is reportedly so trivial that a single hacker could take down large chunks of the internet in a single move. All they would need to do is simultaneously crash enough DNS servers to cause a noticeable outage and serious implications for the internet."

Visit CVE-2015-5477 to learn more about this issue.

**Hillstone Networks Makes Declaration of CVE Compatibility**

July 28, 2015

Hillstone Networks declared that its Next Generation Firewall is CVE-Compatible. For additional information about this and other CVE-Compatible products, visit the CVE-Compatible Products and Services section.

**LINKBYNET Makes Declaration of CVE Compatibility**

July 28, 2015

LINKBYNET declared that its vulnerability database and notification service, LBN Watch, is CVE-Compatible. For additional information about this and other CVE-Compatible products, visit the CVE-Compatible Products and Services section.

**Infobyte Networks Makes Declaration of CVE Compatibility**

July 28, 2015

Infobyte LLC declared that its penetration test collaborative integrated development environment (IDE), Faraday, is CVE-Compatible. For additional information about this and other CVE-Compatible products, visit the CVE-Compatible Products and Services section.

**Seven CVE Identifiers Cited in Numerous Security Advisories and News Media References about the Android "Stagefright" Vulnerability**

July 28, 2015

Seven CVE Identifiers — CVE-2015-1538, CVE-2015-1539, CVE-2015-3824, CVE-2015-3826, CVE-2015-3827, CVE-2015-3828, and CVE-2015-3829 — are cited in numerous major advisories, posts, and news media references related to the recent Android "Stagefright" vulnerability, including the following examples:

http://www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks/

https://threatpost.com/android-stagefright-flaws-put-950-million-devices-at-risk/113960

http://www.techspot.com/news/61530-new-android-vulnerability-targets-messaging-platform-nearly-billion.html

http://www.scmagazine.com/critical-remote-code-execution-vulnerabilities-in-stagefright-exploitable-on-95-percent-of-android-devices/article/428786/

http://www.darkreading.com/vulnerabilities---threats/stagefright-android-bug-heartbleed-for-mobile-but-harder-to-patch/d/d-id/1321477

http://pix11.com/2015/07/27/nearly-1-billion-android-phones-could-be-hacked-with-a-text-message/

http://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/

http://www.itworldcanada.com/post/most-android-devices-can-easily-be-hacked-with-mms-file-vendor

http://www.eweek.com/security/android-stagefright-flaw-puts-hundreds-of-millions-of-users-at-risk.html

http://www.morningnewsusa.com/android-phones-can-be-hacked-with-just-1-text-2329872.html

http://www.techworm.net/2015/07/stagefright-attack-it-takes-only-a-single-text-message-to-hack-an-android-smartphone.html

http://www.computerra.ru/129117/stagefright-android-vulnerability/

http://weblogit.net/2015/07/27/stagefright-android-offen-wie-ein-scheunentor-71250/

http://japanese.engadget.com/2015/07/27/android-95-mms/

http://www.heise.de/newsticker/meldung/Android-Smartphones-ueber-Kurznachrichten-angreifbar-2763764.html

Other news articles may be found by searching on "CVE-2015-1538," "CVE-2015-1539," "CVE-2015-3824," "CVE-2015-3826," "CVE-2015-3827," "CVE-2015-3828," and "CVE-2015-3829" using your preferred search engine. Also, the CVE Identifier pages https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1538, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1539, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3824, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3826, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3827, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3828, and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3829 include lists of advisories used as references.

**CVE Mentioned in Article about Chrome Vulnerabilities on eSecurity Planet**

July 23, 2015

CVE is mentioned throughout a July 22, 2015 article entitled "Google Chrome 44 Updates for 43 Vulnerabilities" on eSecurity Planet. The main topic of the article is that the latest update to Google's Chrome web browser fixes 43 vulnerabilities and the monetary rewards Google paid to security researchers for discovering those vulnerabilities.

The CVE IDs cited in this article include: CVE-2015-1286, a Universal Cross Site Scripting (UXSS) vulnerability in the blink rendering engine; CVE-2015-1275, a UXSS vulnerability; CVE-2015-1271, a heap buffer overflow vulnerability; CVE-2015-1280, a "memory corruption vulnerability in the skia 2D graphics library engine"; CVE 2015-1274, which allowed "allowed executable files to run immediately after download"; and CVE-2015-1288, which "found that in Chrome, spell checking dictionaries could be fetched over HTTP. Generally speaking, Google prefers HTTPS, encrypted HTTP everywhere to prevent man-in-the-middle attacks."

In addition, Google is a CVE Numbering Authority (CNA), assigning CVE IDs for Chrome, Chrome OS, and Android Open Source Project issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs to newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

Visit CVE-2015-1286, CVE-2015-1275, CVE-2015-1271, CVE-2015-1280, CVE-2015-1274, and CVE-2015-1288 to learn more about these issues.

**CVE Identifier "CVE-2015-2426" Cited in Numerous Security Advisories and News Media References about a Zero-Day Microsoft Windows Vulnerability**

July 23, 2015

"CVE-2015-2426" is cited in numerous major advisories, posts, and news media references related to the recent zero-day Microsoft Windows vulnerability, including the following examples:

http://www.computerworld.com/article/2949589/malware-vulnerabilities/microsoft-patches-windows-zero-day-found-in-hacking-teams-leaked-docs.html

http://www.computerweekly.com/news/4500250271/Microsoft-issues-emergency-fix-for-Windows-flaw

http://www.scmagazineuk.com/microsoft-out-of-band-update/article/427507/

https://threatpost.com/microsoft-issues-critical-out-of-band-patch-for-all-versions-of-windows/113866

http://www.scmagazine.com/microsoft-updates-address-opentype-font-driver-vulnerability/article/427424/

http://www.darkreading.com/vulnerabilities---threats/hacking-team-detection-tools-released-by-rook-facebook/d/d-id/1321402

http://www.theregister.co.uk/2015/07/20/windows_microsoft_emergency_patch/

http://www.networkworld.com/article/2949910/microsoft-subnet/microsoft-issues-critical-out-of-band-patch-for-flaw-affecting-all-windows-versions.html

http://www.zdnet.com/article/microsoft-releases-emergency-patch-for-critical-windows-flaw/

http://mnrdaily.com/article/microsoft.patches.windows.zero.day.security.flaw/1448.htm

http://www.biztekmojo.com/00975/patch-opentype-exploit-hacking-team-leak-launched-quickly-microsoft

http://www.itpro.co.uk/data-loss-prevention/25014/microsoft-issues-emergency-software-patch-one-week-ahead-of-windows-10

http://www.ipa.go.jp/security/ciadr/vul/20150721-ms.html

http://techpp.com/2015/07/21/microsoft-security-update-font/

http://hitech.vesti.ru/news/view/id/7362

http://www.digi.no/sikkerhet/2015/07/21/kritisk-hull-i-alle-windows-versjoner

http://de.ubergizmo.com/2015/07/21/hacking-team-microsoft-versorgt-nutzer-mit-notfall-patch.html

Other news articles may be found by searching on "CVE-2015-2426" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2426 includes a list of advisories used as references.

**CVE Mentioned in Article about Oracle's Quarterly Critical Patch Update and a Zero-Day Fix on Computerworld**

July 23, 2015

CVE is mentioned in a July 15, 2015 article entitled "Oracle fixes zero-day Java flaw and over 190 other vulnerabilities" on Computerworld. The main topic of the article is that "Oracle's latest patch, released Tuesday, fixes 25 vulnerabilities in the aging platform, including one that's already being exploited in attacks. In addition to Java, Oracle also updated a wide range of other products, fixing a total of 193 vulnerabilities, 44 stemming from third-party components."

CVE is mentioned with regard to the zero-day vulnerability, as follows: "The most high-risk vulnerability fixed in this Java update is known as CVE-2015-2590 and had zero-day status until this update. This means attackers were already exploiting it while no fix was available."

In addition, Oracle is a CVE Numbering Authority (CNA), assigning CVE IDs for Oracle issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs to newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

Visit CVE-2015-2590 to learn more about the issue cited above.

**CVE Mentioned in Article about Adobe, Microsoft, and Oracle Zero-Day Vulnerabilities on eWeek**

July 23, 2015

CVE is mentioned in a July 15, 2015 article entitled "Adobe, Microsoft and Oracle Patch for Hacking Team Flaws" on eWeek. The main topic of the article is that "In a rare confluence of scheduling and circumstances, Adobe, Microsoft and Oracle issued patches on July 14 for vulnerabilities first publicly revealed July 5 in the breached documents of security firm Hacking Team."

CVE is mentioned regarding Adobe when the author states: "Adobe's Patch Tuesday update includes fixes for the CVE-2015-5122 and CVE-2015-5123 zero-day vulnerabilities that FireEye and Trend Micro found in the Hacking Team materials … Adobe is also updating Adobe Reader and Acrobat for 46 identified CVEs, 27 of which were reported to Adobe by researchers working with Hewlett-Packard's Zero Day Initiative. The new Adobe updates are in addition to the 36 CVEs the company patched on July 8. They included one additional zero-day derived from the Hacking Team breach."

CVE is mentioned regarding Oracle when the author states: "Oracle's July Critical Patch Update (CPU) eclipses Adobe's CVE count, with a staggering 193 unique CVEs identified and fixed. Among them is CVE-2015-2590, which is a zero-day flaw in Java identified by Trend Micro from the Hacking Team breach. The CVE-2105-2590 zero-day in Java is one of 25 patches Oracle is making this month for Java. Trend Micro first discovered CVE-2015-2590 being actively exploited as part of a hacker campaign it has identified as Operation Pawn Storm … In addition to the

Java patches, Oracle's patch haul includes 10 fixes for the Oracle Database, 25 patches in Oracle Berkeley DB and 39 patches for Oracle Fusion Middleware.

CVE is mentioned regarding Microsoft when the author states: "Microsoft is also tackling a vulnerability first revealed in the Hacking Team breach with CVE-2015-2425, a flaw in the Internet Explorer 11 Web browser … Microsoft credits security researchers Bill Finlayson of Vectra Networks, Dhanesh Kizhakkinan of FireEye and Peter Pi of TrendMicro for reporting the CVE-2015-2425 flaw. The CVE-2015-2425 flaw is one of 29 CVEs that Microsoft is patching in IE with its MS15-065 security bulletin."

Adobe, Oracle, and Microsoft are all CVE Numbering Authorities (CNAs), assigning CVE IDs for their own OS and product issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs to newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

Visit CVE-2015-5122, CVE-2015-5123, CVE-2015-2590, and CVE-2015-2425 to learn more about these issues.

**25 CVE IDs Cited in Article about Fixes to Apple OS X and iOS Vulnerabilities on eWeek**

July 7, 2015

Twenty-five CVE IDs are cited in a July 1, 2015 article entitled "Apple Fixes OS X and iOS Flaws Ahead of New Releases" on eWeek. The main topic of the article is that "Apple released the OS X 10.10.4 and iOS 8.4 updates on June 30, providing users with security patches fixing multiple vulnerabilities across both desktop and mobile operating systems" in advance of "new version releases [of its desktop and mobile operating systems] set to debut later this year."

The CVE IDs cited in this article include: CVE-2015-3671, CVE-2015-3672, and CVE-2015-3673 in Apple's Admin framework; CVE-2015-3679, CVE-2015-3680, CVE-2015-3681, and CVE-2015-3682 in Apple Type Services (ATS); CVE-2015-1157, CVE-2015-3685, CVE-2015-3686, CVE-2015-3687, CVE-2015-3688, and CVE-2015-3689 in the CoreText library; CVE-2015-3695, CVE-2015-3696, CVE-2015-3697, CVE-2015-3698, CVE-2015-3699, CVE-2015-3700, CVE-2015-3701, and CVE-2015-3702 in the Intel graphics driver used in OS X; CVE-2015-4000 (also known as "Logjam") in the coreTLS library; CVE-2015-3678, a vulnerability in Apple's high-speed Thunderbolt interface; and, for iOS 8.4, CVE-2015-3726 in the core telephony component and CVE-2015-3728 for WiFi connectivity.

In addition, Apple is a CVE Numbering Authority (CNA), assigning CVE IDs for Apple issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

**CVE Identifier "CVE-2015-3113" Cited in Numerous Security Advisories and News Media References about a Zero-Day Adobe Flash Vulnerability**

July 7, 2015

"CVE-2015-3113" is cited in numerous major advisories, posts, and news media references related to the recent zero-day Adobe Flash vulnerability, including the following examples:

http://ccm.net/news/26353-adobe-releases-urgent-flash-update

http://www.computerweekly.com/news/4500248673/Adobe-patches-Flash-Player-vulnerability-CVE-2015-3113

http://www.techtimes.com/articles/63254/20150624/adobe-releases-patch-to-plug-flash-players-zero-day-vulnerability.htm

http://www.pcworld.com/article/2939552/adobe-patches-zeroday-flash-player-flaw-used-in-targeted-attacks.html

http://arstechnica.com/security/2015/06/patch-early-patch-often-adobe-pushes-emergency-fix-for-active-0-day/

http://www.digitaltrends.com/computing/new-adobe-flash-flaw-allows-remote-takeover-patch-issued/

http://www.eweek.com/security/adobe-fixes-another-zero-day-flaw-in-its-flash-player.html

http://www.winbeta.org/news/emergency-adobe-flash-security-update-rolling-out-windows-linux-and-mac

http://www.itpro.co.uk/security/24853/latest-adobe-flash-vulnerability-appears-in-exploit-kits

http://www.zdnet.com/article/flash-zero-day-flaw-exploited-in-the-wild-users-advised-to-update/

http://www.theinquirer.net/inquirer/news/2414694/adobe-issues-emergency-patch-for-flash-player-zero-day-flaw

https://www.powerpage.org/adobe-pushes-flash-player-18-0-0-194-cites-security-vulnerabilities-in-previous-versions/

http://techreport.com/news/28527/hackers-are-exploiting-a-new-flash-vulnerability

http://www.scmagazine.com/apt-group-exploits-adobe-flash-player-zero-day-in-phishing-operation/article/422352/

http://www.v3.co.uk/v3-uk/news/2414637/adobe-releases-emergency-zero-day-flaw-fix-to-combat-apt3-clandestine-wolf-hackers

http://news.softpedia.com/news/adobe-fixes-flash-player-zero-day-exploited-in-the-wild-485066.shtml

http://www.theregister.co.uk/2015/06/23/adobe_flash_player/

http://www.infosecurity-magazine.com/news/adobe-patches-critical-flash-flaw/

http://enterpriseinnovation.net/article/singapore-based-cyber-security-team-reveals-china-based-threat-group-1115225494

http://www.scmagazineuk.com/time-to-abandon-flash-hit-by-zero-day-once-again/article/422475/

http://www.theregister.co.uk/2015/06/29/ransomware_exploit_kit_slinger_exploits_flash_remote_code_execution/

Other news articles may be found by searching on "CVE-2015-3113" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3113 includes a list of advisories used as references.

**CVE Mentioned in Article about Firefox Vulnerabilities on eWeek**

July 7, 2015

CVE is mentioned in a July 6, 2015 article entitled "Mozilla Fixes Flaws With Firefox 39, Previews Firefox 40" on eWeek. CVE is mentioned when the author states: "As part of the Firefox 39 release, Mozilla is providing 13 security advisories, four of which are rated as being critical. The critical security advisories include MSFA-2015-66 , which provides a patch for seven different identified vulnerabilities (CVE-2015-2734, CVE-2015-2735, CVE-2015-2736, CVE-2015-2737, CVE-2015-2738, CVE-2015-2739 and CVE-2015-2740). "These [vulnerabilities] included three uses of uninitialized memory, one poor validation leading to an exploitable crash, one read of unowned memory in zip files, and two buffer overflows," Mozilla warns in its security advisory. "These do not all have clear mechanisms to be exploited through web content but are vulnerable if a mechanism can be found to trigger them.""

Visit CVE-2015-2734, CVE-2015-2735, CVE-2015-2736, CVE-2015-2737, CVE-2015-2738, CVE-2015-2739, and CVE-2015-2740 to learn more about these issues.

**CVE Mentioned in Article about Drupal Vulnerabilities on Naked Security**

July 7, 2015

CVE is mentioned in a June 19, 2015 article entitled "Drupal flicks fix to nix OpenID admin account hijack hole: Verisign, LiveJournal and StackExchange members are your unknown admins" on Naked Security. CVE is first mentioned at the begging of the article when the author states: "Drupal has shuttered a flaw in its implementation of OpenID that allows attackers to log in as web site administrators. The flaw (CVE-2015-3234) is the most critical of four and affects versions six and seven of the content management system. Drupal's security team say attackers can target unpatched systems if they hold an OpenID account."

CVE is mentioned again when the author states: "Less critical flaws include one (CVE-2015-3232) affecting websites that use the Drupal 7 Field ID module which attackers can use to redirect users to malicious web properties. Another (CVE-2015-3233) relates to poor validation checks in the overlay module leading to another open direct hole for sites that have enabled the 'access the administrative overlay' permission which will overlay pages as Javascript. The final vulnerability (CVE-2015-3231) is in an information disclosure hole in Drupal 7 that could cache sensitive data then viewable by a non-priveleged primary user (user 1)."

Visit CVE-2015-3231, CVE-2015-3232, CVE-2015-3233, and CVE-2015-3234 to learn more about these issues.

**CVE List Surpasses 70,000 CVE IDs**

June 26, 2015

The CVE website now contains 70,036 unique cyber 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. Cyber security professionals and product vendors from around the world use CVE Identifiers (CVE IDs) as a standard method for identifying vulnerabilities; facilitating their work processes; and cross-linking among products, services, and other repositories that use the identifiers.

Each of the 70,000+ identifiers on the CVE List includes the following: CVE Identifier number, brief description of the security vulnerability, and pertinent references such as vulnerability reports and advisories.

Visit the CVE List page to download the complete list in various formats or to look-up an individual identifier. Fix information, enhanced searching, and a Common Vulnerability Scoring System (CVSS) calculator for scoring the severity of CVE IDs are available from U.S. National Vulnerability Database (NVD).

**CVE Identifiers Used throughout Trustwave's "2015 Trustwave Global Security Report"**

June 18, 2015

CVE IDs are cited throughout Trustwave's "2015 Trustwave Global Security Report" to uniquely identify the vulnerabilities referenced in the report text and several of the charts.

CVE was also specifically mentioned in a section of the report that discussed "Celebrity Vulnerabilities' such as "Heartbleed," "Shellshock," "Poodle," and others. The report states: "For the purpose of this discussion, we define "celebrity" vulnerabilities as those such as Heartbleed that receive memorable names, and sometimes logos, from their discoverers. For years, researchers have assigned quirky names to the malware they discover - for example, the Melissa virus. Catch names and logos can help spread the word more quickly, and in 2014 this trend extended beyond malware to vulnerabilities. Prior, the security community generally referenced flaws with the Common vulnerabilities and Exposures (CVE) numbering standard (e.g., CVE-2014-0160). In 2014, a number of celebrity vulnerabilities made headlines. Higher-profile promotion of security weaknesses no doubt led to quicker patching among businesses."

The free report is available for download at https://www2.trustwave.com/GSR2015.html?utm_source=webbanner&utm_medium=web&utm_campaign=GSR. You must fill-out a form to download the report.

**CVE Identifier "CVE-2015-2865" Cited in Numerous Security Advisories and News Media References about the Samsung Galaxy Keyboard Vulnerability**

June 18, 2015

NOTICE: The CVE Identifier cited in this article, "CVE-2015-2865", has since been marked as a REJECT because "this ID was intended for one issue, but was associated with two issues." All CVE users should instead consult CVE-2015-4640 and CVE-2015-4641 regarding the Samsung Galaxy keyboard vulnerabilities.

"CVE-2015-2865" is cited in numerous major advisories, posts, and news media references related to the recent Samsung Galaxy keyboard vulnerability, including the following examples:

http://www.computerworld.com/article/2936613/cybercrime-hacking/vulnerability-in-samsung-galaxy-phones-put-over-600-million-samsung-phone-users-at-risk.html

http://www.scmagazine.com/nowsecure-discloses-samsung-swift-keyboard-vulnerability/article/421288/

https://fortune.com/2015/06/17/samsung-galaxy-keyboard-bug/

http://arstechnica.com/security/2015/06/new-exploit-turns-samsung-galaxy-phones-into-remote-bugging-devices/

http://techfrag.com/2015/06/17/samsung-devices-vulnerable-hackers-attacks/

http://www.military-technologies.net/2015/06/17/samsung-cellphone-keyboard-software-vulnerable-to-attack/

http://www.lemondeinformatique.fr/actualites/lire-600-millions-de-mobiles-samsung-victimes-de-la-faille-swiftkey-61503.html

http://www.silicon.de/41613510/600-millionen-android-smartphones-von-leck-gefaehrdet/

http://www.elgrupoinformatico.com/millones-moviles-samsung-peligro-por-una-vulnerabilidad-swiftkey-t23773.html

http://indianexpress.com/article/technology/mobile-tabs/samsung-devices-have-keyboard-security-risk-over-600-mn-devices-affected-report/

http://news.softpedia.com/news/Over-600-Million-Samsung-Devices-Vulnerable-to-Keyboard-Security-Risk-484562.shtml

http://thetechportal.in/2015/06/17/swiftkey-vulnerability-in-samsung-galaxy-phones-puts-600-mn-devices-at-risk/

http://techreport.com/news/28479/updated-preinstalled-swiftkey-app-can-own-some-samsung-phones

http://www.infosecurity-magazine.com/news/keyboard-vulnerability-600-million/

Other news articles may be found by searching on "CVE-2015-2865" using your preferred search engine. Also, the CVE Identifier pages https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4640 and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4641 include lists advisories used as references.

**CVE IDs Used throughout Qualys' Top 10 External and Top 10 Internal Vulnerabilities Lists**

June 3, 2015

CVE IDs are used throughout Qualys, Inc.'s February 2015 "Top 10 Vulnerabilities" lists to uniquely identify the vulnerabilities referenced on its top 10 external and top 10 internal vulnerabilities lists. The two lists are "dynamic lists of the most prevalent and critical security vulnerabilities in the real world."

According to the Qualys website, the two lists are "Based on the Laws of Vulnerabilities, this information is computed anonymously from over 1 billion IP audits per year. The Top 10 External Vulnerabilities are the most prevalent and critical vulnerabilities which have been identified on Internet facing systems. The Top 10 Internal Vulnerabilities show this information for systems and networks inside the firewall."

Review Qualys's Top 10 External Vulnerabilities and Top 10 Internal Vulnerabilities lists at: https://www.qualys.com/research/top10/.

**CVE Identifier "CVE-2015-1835" Cited in Numerous Security Advisories and News Media References about the Apache Cordova Android Vulnerability**

June 3, 2015

"CVE-2015-1835" is cited in numerous major advisories, posts, and news media references related to the recent Apache Cordova Android vulnerability, including the following examples:

http://www.techworm.net/2015/06/security-bug-in-cordova-allows-a-single-url-click-to-tamper-android-apps.html

http://www.scmagazine.com/apache-cordova-patches-application-vulnerability/article/417257/

http://www.zdnet.com/article/security-vuln-allows-android-app-tampering-through-single-url-click/

http://www.v3.co.uk/v3-uk/news/2410427/apache-cordova-flaw-leaves-one-in-20-android-apps-open-to-attack

http://www.securityweek.com/serious-flaw-apache-cordova-puts-android-apps-risk

http://news.softpedia.com/news/Apache-Cordova-Glitch-Allows-Tampering-with-Mobile-App-Behavior-482561.shtml

http://searchsecurity.techtarget.com/news/4500247192/Smartphone-security-threats-plague-Android-and-iPhone-alike

http://securityaffairs.co/wordpress/37286/hacking/flaw-cordova-api-framework.html

http://darkmatters.norsecorp.com/tag/apache-cordova/

http://securitygladiators.com/2015/05/29/apache-cordova-vulnerability-lets-hackers-change-apps-behavior/

http://www.techsupportforum.com/forums/f90/trend-micro-discovers-apache-cordova-vulnerability-that-allows-one-click-modification-1000193.html

http://www.hackbusters.com/news/stories/329977-vulnerability-in-cordova-android-platform-allows-for-app-behavior-modification

http://www.pressebox.de/pressemitteilung/trend-micro-deutschland-gmbh/Jede-20-Android-App-verwundbar-Trend-Micro-warnt-vor-Sicherheitsluecke-in-Apache-Cordova/boxid/740959

http://japan.zdnet.com/article/35065196/

http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-apache-vulnerability-that-allows-one-click-modification-of-android-apps/

Other news articles may be found by searching on "CVE-2015-1835" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1835 includes a list of advisories used as references.

**CVE Mentioned in Article about Approaches to Vulnerability Naming on Christian Science Monitor**

May 28, 2015

CVE is mentioned in a May 22, 2015 article entitled "What the security industry can learn from the World Health Organization" on Christian Science Monitor. The main topic of the article is about how the "discovery of computer bugs can be marketing boons for cybersecurity firms. But one critic says the industry should take a page from the health profession and select names for flaws that aren't designed to stoke fear or generate buzz."

The author then discusses how some of the recent named bugs have been more about marketing and less about how serious they are, such as "VENOM," (i.e., CVE-2015-3456) which National Vulnerability Database ranks "…between medium and high risk – a 7.5 out of 10. But this year alone, it has listed nearly 800 bugs as high risk, and there is no shortage of 10s. Many of those involve extraordinarily popular software programs such major operating systems and Web browsers."

The article also includes a quote from Chris Eng, vice president of research at Veracode, who says: "What ends up happening is named vulnerabilities get more attention regardless of how much they deserve it. The intuition is, if it's branded, it's more dangerous."

The author continues: "Mr. Eng suggests that, in an ideal world, the industry could go back to the old days, and refer to vulnerabilities by their Common Vulnerabilities and Exposures numbers. "They're only eight numbers," he says. "They aren’t that hard to remember. And the first four are the year."

Visit CVE-2015-3456 to learn more about "VENOM."

**CVE Mentioned in Article about "Logjam" Vulnerability on SecurityWeek**

May 28, 2015

CVE was mentioned in a May 21, 2015 article entitled "Hundreds of Cloud Services Potentially Vulnerable to Logjam Attacks: Skyhigh" on SecurityWeek. The main topic of the article is the "Logjam vulnerability, which is similar to the FREAK bug, is caused due to the way the Diffie-Hellman (DHE) key exchange has been deployed. The flaw can be exploited by a man-in-the-middle (MitM) attacker to downgrade TLS connections to weak, export-grade crypto, and gain access to the data passing through the connection."

CVE is mentioned when the author states: "Logjam (CVE-2015-4000) affects all servers that support 512-bit export-grade cryptography and all modern web browsers, for which patches are being released. The vulnerability initially affected over 8 percent of the top 1 million HTTPS websites, and more than 3 percent of the browser trusted sites."

Visit CVE-2015-4000 to learn more about "Logjam."

**CVE Mentioned in Article about Vulnerabilities in Hospira Drug Pumps on SC Magazine**

May 28, 2015

CVE was mentioned in a May 14, 2015 article entitled "DHS adds more bug disclosures to Hospira drug pump alert, FDA joins call" on SC Magazine. The main topic of the article is warnings by the U.S. Department of Homeland Security and U.S. Food and Drug Administration (FDA) that "[Hospira] infusion pumps were vulnerable to remotely exploitable bugs."

CVE is mentioned when the author states: "Last Tuesday, DHS' ICS-CERT told Hospira LifeCare PCA Infusion System users that an improper authorization flaw and insufficient verification of data authenticity vulnerability affected the product. But, on Wednesday, the CERT decided to amend its advisory to include more vulnerabilities afflicting versions 5 and 3 of the drug pumps. In a Wednesday blog post, Patrick Coyle, a chemical security and cybersecurity expert in Texas, explained that the updated DHS alert followed his and OXTECH Security's warnings about other vulnerabilities which could allow hardcoded passwords to be used for device access (CVE-2015-1011), and exposed sensitive information, like stored credentials, to unauthorized parties in clear text (CVE-2015-1012)."

CVE is mentioned a second time when the author states: "The hardcoded password issue (CVE-2015-1011) was assigned a CVSS (Common Vulnerability Scoring System) base score of 10, and the bug allowing clear text storage of sensitive information (CVE-2015-1012) was assigned a base score of 6.4."

Visit CVE-2015-1011 and CVE-2015-1012 to learn more about the issues cited above.

**CVE Mentioned in Article about a Vulnerability Affecting "Millions" of Routers and IoT Devices on ZDNet**

May 28, 2015

CVE is mentioned in a May 20, 2015 article entitled "NetUSB flaw leaves 'millions' of routers, IoT devices vulnerable to hacking" on ZDNet. The main topic of the article is that "Potentially millions of routers and Internet-of-Things devices have been placed at risk of hijacking due to a stack buffer overflow security flaw."

CVE is mentioned when the author states: "…the vulnerability,CVE-2015-3036, allows for an unauthenticated attacker on a local network to trigger a kernel stack buffer overflow which causes denial-of-service or permits remote code execution. In addition, some router configurations may allow remote attacks."

The author also explains how millions of routers and Internet of Things (IoT) devices could be affected: "KCode-developed NetUSB, used in a plethora of popular routers available commercially, is used to provide USB over IP functionality. USB devices including printers and flash drivers, plugged into a Linux-based system, can be granted network access over TCP port 20005 through the technology. Routers, access points and dedicated USB over IP boxes often use this proprietary software."

Visit CVE-2015-3036 to learn more about the issue cited above.

**CVE Mentioned in Article about WebKit Vulnerabilities in Safari Browser on ThreatPost**

May 28, 2015

CVE is mentioned throughout a May 27, 2015 article entitled "Apple Fixes WebKit Vulnerabilities in Safari Browser" on ThreatPost. The main topic of the article is that "Apple has updated its Safari browser, fixing a handful of exploitable WebKit flaws in various versions of Safari. WebKit is the core layout engine responsible for rendering webpages in the Safari browser."

CVE is first mentioned when the author states: "The first bulletin, vulnerabilities uncovered by Apple, resolves multiple memory corruption issues in Webkit. On unpatched systems, an attacker could exploit CVE-2015-1152, CVE-2015-1153 and CVE-2015-1154 by compelling a user to visit a malicious website, which, in turn, could lead to an unexpected application termination or arbitrary code execution. Apple resolved the problem with improved memory handling."

CVE is mentioned a second time when the author states: "The second bulletin resolves just one vulnerability, CVE-2015-1155, which …emerged from a state management problem in Safari that allowed unprivileged origins to access filesystem contents. This was exploitable if a user were compelled to visit a specially created webpage, after which the attacker could access filesystem information. Apple resolved this … through improved state management."

Visit CVE-2015-1152, CVE-2015-1153, CVE-2015-1154, and CVE-2015-1155 to learn more about the issues cited above.

**CVE and CVSS Mentioned in SANS' "Cyber Threat Intelligence: Who's Using it and How?" Report**

May 28, 2015

CVE and Common Vulnerability Scoring System (CVSS) are mentioned in the survey results from SANS' s February 2015 "Cyber Threat Intelligence: Who's Using it and How?"report.

CVE and CWSS are cited in a survey respondent quote in the "CTI Standards and Tools" section: "While it is not the biggest issue being encountered, a shortage of standards and interoperability around feeds, context and detection may become more problematic as more organizations add more sources of [Cyber Threat Intelligence (CTI)] into their detection and response programs. Without the proper standardization of CTI feed information, organizations could still miss indicators of compromise.

"Vulnerability data from the infrastructure side and the web application side could be better standardized. CVE and CVSS are great places to start by providing taxonomy and common nomenclature, and they provide a great way to quickly name/categorize a finding so multiple analysts from different organizations are speaking about the same finding/weakness," says David Screws, director of security engineering at Equifax."

Read the full report at https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767.

**CVE Identifier "CVE-2015-3456" Cited in Numerous Security Advisories and News Media References about the VENOM Vulnerability**

May 19, 2015

"CVE-2015-3456" is cited in numerous major advisories, posts, and news media references related to the recent VENOM vulnerability, including the following examples:

http://www.scmagazine.com/oracle-patches-buffer-overflow-bug-venom/article/415329/

http://www.csoonline.com/article/2922066/vulnerabilities/venom-hype-and-pre-planned-marketing-campaign-panned-by-experts.html

https://threatpost.com/venom-flaw-in-virtualization-software-could-lead-to-vm-escapes-data-theft/112772

http://www.darkreading.com/vulnerabilities---threats/experts-opinions-mixed-on-venom-vulnerability/d/d-id/1320425

http://arstechnica.com/security/2015/05/extremely-serious-virtual-machine-bug-threatens-cloud-providers-everywhere/

http://arstechnica.com/security/2015/05/extremely-serious-virtual-machine-bug-threatens-cloud-providers-everywhere/

http://www.esecurityplanet.com/network-security/crowdstrike-warns-of-venom-vulnerability.html

http://www.firstpost.com/business/venom-vulnerability-expose-virtual-machines-unpatched-host-systems-2245614.html

http://mashable.com/2015/05/13/venom-security-faq/

http://fortune.com/2015/05/13/amazon-says-its-cloud-not-bitten-by-venom-flaw/

http://www.theregister.co.uk/2015/05/14/venom_analysis/

http://www.cio.com/article/2922214/critical-vm-escape-vulnerability-impacts-business-systems-data-centers.html

http://www.computerweekly.com/news/4500246265/Venom-is-serious-but-no-Heartbleed-say-experts

http://siliconangle.com/blog/2015/05/14/venom-vulnerability-bites-vm-hosts/

http://www.eweek.com/security/the-venomous-search-for-the-next-heartbleed-and-venom-isnt-it.html

http://www.scmagazine.com/venom-vulnerability-enables-virtual-machine-escapes/article/414549/

http://www.channelpartnersonline.com/blogs/lorna-garey-blog/2015/05/venom-serious-but-no-heartbleed.aspx

http://www.cbronline.com/news/cybersecurity/data/does-the-bite-live-up-to-the-hype-10-insights-into-the-venom-vulnerability-4577567

http://www.itworldcanada.com/post/venom-bug-bites-several-virtualization-platforms-patching-needed

http://www.dailymail.co.uk/sciencetech/article-3080708/Venom-bug-allow-hackers-cloud-servers-experts-say-worse-Heartbleed.html

Other news articles may be found by searching on "CVE-2015-3456" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3456 includes a list of advisories used as references.

**CVE Mentioned in Article about Attackers Exploiting Known but Unpatched Vulnerabilities on TechWeekEurope**

May 19, 2015

CVE is mentioned throughout a May 18, 2015 article entitled "What Can We Learn From Our Cyber Security Mistakes?" on TechWeekEurope. The main topic of the article is how "In the last 12 months the threat landscape expanded into the network infrastructure itself, with a multitude of hidden vulnerabilities revealed deep within the code base of age-old popular protocols like Bash, OpenSSL, SSLv3. The likes of Shellshock, Heartbleed and Poodle highlighted the brittle nature of infrastructure standards and pushed businesses into action to deploy rapid risk assessment and apply mitigation methods to prevent exploitation and data theft."

CVE is mentioned thought the article in reference to the specific vulnerabilities discussed, when the author states: "The first major indication of the fragility in existing infrastructures came one year ago with the OpenSSL Heartbleed vulnerability (CVE-2014-0160). Heartbleed exposed the memory of systems using vulnerable versions of OpenSSL." "Five months later, in September 2014, IT teams already reeling from Heartbleed had to face up to the even bigger challenge of mitigating Bash Shellshock (CVE-2014-6271). The 25-year-old vulnerability allowed for remote execution of arbitrary commands via crafted environment variables. Within days of the public announcement, proof-of-concept code was widely published and attackers were dropping malware onto vulnerable servers." "A few weeks later the SSLv3 Poodle (CVE-2014-3566) weakness surfaced, posing a serious data theft risk to secure communications using the SSL standard. This also highlighted widespread use of older standards, even while newer and more secure standard options were available."

The author concludes the article by stating: "Businesses must ensure they conduct regular reviews of their mission-critical systems using legacy technologies for potential risk and upgrade opportunities … Security professionals must also ensure they stay up to date with streams of threat intelligence and conversations that will reveal newly discovered potential vulnerabilities, by subscribing to security news feeds, reading blogs and networking with peers at any opportunity."

Visit CVE-2014-0160 to learn about "Heartbleed"; CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, and CVE-2014-6278 to learn more about "Bash Shellshock"; and CVE-2014-3566 to learn more about "POODLE".

**CVE Identifiers Used throughout Websense's "Threat Report 2015"**

May 7, 2015

CVE IDs are mentioned throughout Websense, Inc.'s "Threat Report 2015" to uniquely identify many of the vulnerabilities referenced in the report text.

According to Websense's Websense 2015 Threat Report: Cybercrime Gets Easier, Attribution Gets Harder, Quality over Quantity and Old becomes the New press release on April 8, 2015, the report "looks at how threat actors are gaining capabilities through the adoption of cutting-edge tools instead of technical expertise. Redirect chains, code recycling and a host of other techniques are allowing these actors to remain anonymous, making attribution time consuming, difficult and ultimately unreliable. Widespread use of older standards in lieu of newer and more secure options continues to leave systems vulnerable and exposed. A brittle infrastructure allows threats to expand into the network framework itself, including the code base of Bash, OpenSSL, and SSLv3."

According to the press release, "In 2014, 99.3 percent of malicious files used a Command & Control URL that has been previously used by one or more other malware samples. In addition, 98.2 percent of malware authors used C&C's found in five other types of malware."

The report also states that "Threat actors are blending old tactics, such as macros, in unwanted emails with new evasion techniques. Old threats are being "recycled" into new threats launched through email and web channels, challenging the most robust defensive postures. Email, the leading attack vector a decade ago, remains a very potent vehicle for threat delivery, despite the now dominant role of the web in cyberattacks. For example: In 2014, 81 percent of all email scanned by Websense was identified as malicious. This number is up 25 percent against the previous year. Websense also detected 28 percent of malicious email messages before an anti-virus signature became available."

The free report is available for download at http://www.websense.com/content/websense-2015-threat-report.aspx?intcmp=hp-promo-en-2015-threat-report.

**CVE Identifiers Used throughout F-Secure's "Threat Report 2014"**

April 29, 2015

CVE IDs are mentioned throughout F-Secure's "Threat Report H2 2014" to uniquely identify many of the vulnerabilities referenced in the report text. According to F-Secure's New F-Secure Report Warns of Growth in Extortion Malware press release on April 23, 2015, the report describes how "New research from cyber security firm F-Secure points to an increase in the amount of malware designed to extort money from unsuspecting mobile phone and PC users. According to the new Threat Report, malware such as premium SMS message sending trojans and ransomware continue to spread, making them a notable presence in today's digital threat landscape."

According to the press release, "259 out of the total 574 known variants of the SmsSend family were identified in the latter half of 2014, making it the fastest growing family of mobile malware. SmsSend generates profits for criminals by infecting Android devices with a trojan that sends SMS messages to premium-rate numbers. Ransomware also continued to plague mobile users, with the Koler and Slocker families of ransomware identified as the top threats to Android devices."

The report also provides a top 10 malware list for PCs for the second half of 2014. As stated in the press release, "PCs also saw an increase in ransomware detections, with the Browlock ransomware family entering the top 10 threats identified in the report. Other notable threats in the top 10 include more established malware families, such as the Conficker/Downadup worm, the Sality virus, and the various strains of the Ramnit virus. These three families collectively account for 55% of the total detections in the top 10 list."

The free report is available for download at https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2014.

**CVE Mentioned in "How to Get the CVSS Right" Article on Dell's Tech Page One Blog**

April 23, 2015

CVE and CVSS are the main topics of an April 17, 2015 article entitled "How to Get the CVSS Right" on Dell's Tech Page One Blog. The main topic of the article is how to use the "Common Vulnerability Scoring System (CVSS) … a free and open industry standard for assessing the severity of computer system security vulnerabilities. Currently in version 2, with an update in version 3 in development, CVSS attempts to establish a measure of how much concern a vulnerability warrants, compared to other vulnerabilities, so efforts can be prioritized. The scores are based on a series of measurements, called metrics. The scores range from 0 to 10. High vulnerabilities are those with a base score in the range 7.0-10.0, medium in 4.0-6.9 and 0-3.9 are low."

CVE is mentioned at the beginning of the article, when the author states: "For anyone dealing with software vulnerabilities, the CVE and CVSS are often their first stops in finding out the scope and details, and just about everything else they need to know about the specific vulnerability."

A CVSS calculator for scoring CVE IDs is available on the U.S. National Vulnerability Database at https://nvd.nist.gov/cvss.cfm?calculator&adv&version=2#score.

**CVE Mentioned throughout Article about Verizon's "2015 Data Breach Investigations Report" on Computerworld**

April 23, 2015

CVE is mentioned in an April 15, 2015 article entitled "90% of security incidents trace back to PEBKAC and ID10T errors" on Computerworld. The main topic of the article is that "90% of security incidents are still caused by [problem exists between keyboard and chair (PEBKAC)] and ID10T errors, according to Verizon's 2015 Data Breach Investigations Report. Phishing attacks are a prime example of how the problem exists between keyboard and user as the DBIR said it takes a mere one minute and 22 seconds after a phishing email is sent before the first victim clicks on the tainted link."

CVE is first mentioned when the author states: "According to the report, "99.9% of the exploited vulnerabilities had been compromised more than a year after the associated CVE was published." It's a mistake for any vulnerability management program to ignore the really old CVEs (Common Vulnerabilities and Exposures) since some successful cyberattacks in 2014 exploited vulnerabilities dating back to 1999. A good vulnerability management program should include a "broad coverage of the 'oldies but goodies.' Just because a CVE gets old doesn't mean it goes out of style with the exploit crowd."

CVE is mentioned again when the author quotes the report, as follows: "Ten CVEs account for almost 97% of the exploits observed in 2014," the report states. "While that's a pretty amazing statistic, don't be lulled into thinking you've found an easy way out of the vulnerability remediation rodeo. Prioritization will definitely help from a risk-cutting perspective, but beyond the top 10 are 7 million other exploited vulnerabilities that may need to be ridden down."

CVE is mentioned a third time, as follows: "Yet Verizon pointed out that other than the CVSS (Common Vulnerability Scoring System) score, there is another attribute of a "critical" vulnerability. "If a vulnerability gets a cool name in the media, it probably falls into this 'critical vulnerability' label." Examples from 2014 included Heartbleed, POODLE, Schannel and Sandworm – all of which were "exploited within a month of CVE publication date."

**CVE Mentioned in Article about Verizon's "2015 Data Breach Investigations Report" on eWeek**

April 23, 2015

CVE is mentioned in an April 14, 2015 article entitled "Verizon Data Breach Study Finds Little Change in Attack Patterns" on eWeek. The main topic of the article is that "Verizon's 2015 Data Breach Investigations Report (DBIR), released today, finds that little has changed in the threat landscape since the 2014 report came out. Overall, the 2015 DBIR received data from 79,790 security events, of which 2,122 were confirmed data breaches. In contrast, the 2014 report was based on data upon 63,437 security incidents, of which 1,367 were confirmed data breaches. As was the case in the 2014 report, Verizon has identified nine basic attack patterns into which nearly all attacks can be categorized: point-of-sale (POS) intrusions, Web application attacks, insider misuse, theft and loss, miscellaneous errors, crimeware, payment-card skimmers, denial-of-service attacks and cyber-espionage."

CVE is mentioned at the conclusion of the article, when the author states: "Verizon's analysis also shows that not every vulnerability is exploited. There are some 67,567 vulnerabilities with a CVE (Common Vulnerabilities and Exposures) designation, but only 792 of them were exploited in 2014."

**CVE Mentioned in Article about Oracle's Quarterly Critical Patch Update on Application Development Trends Magazine**

April 23, 2015

CVE is mentioned in an April 17, 2015 article entitled "Oracle Releases 14 Java Security Patches, Last Patch Update for Java 7" on Application Development Trends Magazine. The main topic of the article is that "Oracle's latest quarterly Critical Patch Update (CPU) includes 98 fixes for vulnerabilities in Oracle products, including 14 that address Java SE issues."

CVE is mentioned at the beginning of the article, as follows: "Three of the Java vulnerabilities identified (CVE-2015-0469, CVE-2015-0459, and CVE-2015-0491), earned a CVSS score of 10.0, the highest, and thus, the most severe on that scale. Vulnerabilities of that level of severity can be exploited over the network without authentication and can lead to a full compromise of the system's confidentiality and integrity. Oracle uses the Common Vulnerability Scoring System (CVSS) to provide an open and standardized rating of the security holes it finds in its products."

In addition, Oracle is a CVE Numbering Authority (CNA), assigning CVE IDs for Oracle issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

Visit CVE-2015-0469, CVE-2015-0450, and CVE-2015-0491 to learn more about the issues cited above.

**CVE Identifier "CVE-2015-3043" Mentioned in Article about an Adobe Zero-Day Vulnerability on CSO**

April 23, 2015

CVE is mentioned in an April 15, 2015 article entitled "Adobe patches vulnerabilities in ColdFusion, Flex and Flash Player, including a zero-day flaw" on CSO. The main topic of the article is that "Adobe Systems released security patches Tuesday for ColdFusion, Flex and Flash Player, the latter addressing a flaw for which is an exploit is already available."

CVE is mentioned when the author states: "One of the flaws, tracked as CVE-2015-3043 in the Common Vulnerabilities and Exposures (CVE) database, has been known by attackers since before Adobe released its latest patches. This makes it a so-called zero-day vulnerability -- a flaw for which a fix was not yet available when it began being exploited. "Adobe is aware of a report that an exploit for CVE-2015-3043 exists in the wild, and recommends users update their product installations to the latest versions," the company said in a security advisory."

Visit CVE-2015-3043 to learn more about the issue cited above.

**CVE Mentioned in Article about Microsoft's Patch Tuesday for April on SC Magazine**

April 23, 2015

CVE is mentioned in an April 14, 2015 article entitled "Microsoft addresses 26 vulnerabilities, some critical, on Patch Tuesday" on SC Magazine. CVE is first mentioned in a quote by Qualys, Inc. CTO Wolfgang Kandek, who states: "CVE-2015-1641 is [a remote code execution] 0-day and is currently under limited attacks in the wild on Word 2010. It applies equally to Word 2007, 2012 and even to Word 2011 on the Mac. Microsoft rates it only "important" because the exploit requires the user to open a malicious file."

CVE is mentioned again when the author states: "Two other critical remote code execution vulnerabilities addressed in the Office bulletin are CVE-2015-1649 and CVE-2015-1651, which Kandek wrote are triggered in Office 2007 and Office 2010 by simply looking at an email in the Outlook preview pane. Another critical bulletin addresses a vulnerability in the HTTP protocol stack – CVE-2015-1635 – that can enable remote code execution if an attacker sends a specially crafted HTTP request to an affected Windows system, according to a Tuesday release. Windows 7, Windows 8 and 8.1, Windows Server 2008 R2, and Windows Server 2012 and Windows Server 2012 R2 are affected."

CVE is mentioned a third time, when the author states: "The final critical bulletin addresses a vulnerability – CVE-2015-1645 – that can allow for remote code execution if a user browses to a specially crafted website, opens a specially crafted file, or browses to a working directory containing a specially crafted Enhanced Metafile image file, the release indicated."

Visit CVE-2015-1641, CVE-2015-1649, CVE-2015-1635, CVE-2015-1651, and CVE-2015-1645 to learn more about the issues cited above.

**CVE Identifiers Used throughout HP's "HP Cyber Risk Report 2015"**

April 23, 2015

CVE IDs are cited throughout Hewlett-Packard Development Company, L.P.'s "HP Cyber Risk Report 2015" to uniquely identify many of the vulnerabilities referenced in the report text and charts. In addition, CVE IDs are a main topic in the "Vulnerabilities and exploits" section of the report, regarding the following discussions: "Top CVE-2014 numbers collected in 2014," "Top CVE-2014 for malware attacks," and “Top CVE numbers seen in 2014."

According to HP's "Security Threat Landscape Still Plagued by Known Issues, says HP" press release issued on February 23, 2015, the report provides "in-depth threat research and analysis around the most pressing security issues plaguing the enterprise during the previous year and indicating likely trends for 2015. Authored by HP Security Research, the report examines the data indicating the most prevalent vulnerabilities that leave organizations open to security risks. This year's report reveals that well-known issues and misconfigurations contributed to the most formidable threats in 2014."

In addition, HP is a CVE Numbering Authority (CNA), assigning CVE IDs for HP issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

The free report is available for download at http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/index.html?jumpid=reg_r1002_usen_c-001_title_r0001. You must fill-out a form to download the report.

**iScan Online Makes Declaration of CVE Compatibility**

April 16, 2015

iScan Online, Inc. declared that its vulnerability detection and financial risk analytics product, Data Breach Risk Intelligence Platform, is CVE-Compatible. For additional information about this and other CVE-Compatible products, visit the CVE-Compatible Products and Services section.

**Interition Makes Declaration of CVE Compatibility**

April 16, 2015

Interition Ltd. declared that its software code knowledge base, Sparqlycode, is CVE-Compatible. For additional information about this and other CVE-Compatible products, visit the CVE-Compatible Products and Services section.

**CVE Identifiers Used throughout Google's "Android Security 2014 Year in Review" Report**

April 10, 2015

CVE IDs are mentioned throughout Google, Inc.'s "Google Report Android Security 2014 Year in Review" to uniquely identify many of the vulnerabilities referenced in the report text. According to Google's Android Security State of the Union 2014 blog post on April 2, 2015, the report "analyzes billions (!) of data points gathered every day during 2014 and provides comprehensive and in-depth insight into security of the Android ecosystem. We hope this will help us share our approaches and data-driven decisions with the security community in order to keep users safer and avoid risk."

Google is a CVE Numbering Authority (CNA), assigning CVE IDs for Chrome, Chrome OS, and Android Open Source Project issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

The free report is available for download at http://googleonlinesecurity.blogspot.com/2015/04/android-security-state-of-union-2014.html.

**CVE Mentioned in Article about a "Critical Backdoor Flaw in OS X 10.10.3" on eWeek**

April 10, 2015

CVE is mentioned in an April 9, 2015 article entitled "Apple Patches Critical Backdoor Flaw in OS X 10.10.3" on eWeek. CVE is first mentioned when the author states: Among the security issues patched in OS X 10.10.3 is a security vulnerability in its administration framework. The issue, identified as CVE-2015-1130, was reported by security researcher Emile Kvarnhammar, CEO at TrueSec. … While Apple has now fixed the CVE-2015-1130 in the 10.10.3 update for users of Apple's Yosemite OS 10.10 operating system, older OS X systems are also at risk."

CVE is mentioned a second time, when the author states: "Apple also has nine patches in OS X 10.10.3 for various OS X kernel vulnerabilities. Among the patched kernel flaws is CVE-2015-1103, which was discovered by Zimperium Mobile Security Labs. According to Apple's advisory, the flaw could have enabled an attacker to redirect user traffic to arbitrary hosts."

CVE is mentioned a third time, when the author states: "Apple is also providing its OS X users with the Safari 8.0.5 update. Seven security updates in the Safari browser are specifically for the WebKit rendering engine. One particularly nasty flaw fixed in Safari is CVE-2015-1129, an SSL/TLS tracking issue. According to Apple, the vulnerability could have enabled users to be tracked by malicious Websites using client certificates."

Visit CVE-2015-1130 and CVE-2015-1129 to learn more about the issues cited above.

**CVE Identifier "CVE-2015-0932" Cited in Numerous Security Advisories and News Media References about a Zero-Day Hotel Wi-Fi Network Vulnerability**

April 10, 2015

"CVE-2015-0932" is cited in numerous major advisories, posts, and news media references related to a zero-day hotel Wi-Fi network vulnerability, including the following examples:

http://www.zdnet.com/article/severe-hotel-wi-fi-network-vulnerability-patched/

https://threatpost.com/hotel-internet-gateways-patched-against-remote-exploit/111829

http://www.pcmag.com/article2/0,2817,2479034,00.asp

http://www.eweek.com/blogs/security-watch/misconfiguration-exposes-hotel-routers-to-risk.html

http://www.esecurityplanet.com/wireless-security/new-security-flaw-found-in-hotel-wi-fi-systems.html

http://www.computerworld.com/article/2902874/popular-hotel-internet-gateway-devices-vulnerable-to-hacking.html

http://www.theregister.co.uk/2015/03/27/hotel_antlabs_inngate_rsync_vulnerability/

http://www.darkreading.com/attacks-breaches/cylance-researchers-discover-critical-vulnerability-affecting-hotel-chains-worldwide/d/d-id/1319644

http://www.networkworld.com/article/2902892/security0/flaw-in-common-hotel-router-threatens-guests-devices.html

http://www.consumeraffairs.com/news/hackers-breach-public-wi-fi-at-multiple-hotels-and-convention-centers-033015.html

http://www.net-security.org/secworld.php?id=18142

http://thehackernews.com/2015/03/hacking-hotel-wifi-network.html

http://www.pcworld.com/article/2903116/popular-hotel-internet-gateway-devices-vulnerable-to-hacking.html

http://www.marketwired.com/press-release/cylance-researchers-discover-critical-vulnerability-affecting-hotel-chains-worldwide-2004120.htm

Other news articles may be found by searching on "CVE-2015-0932" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0932 includes a list of advisories used as references.

**CVE Mentioned in Article about an Exploit Targeting the Middle East Energy Industry on ZDNet**

April 10, 2015

CVE is mentioned in a March 31, 2015 article entitled "Reconnaissance malware wave strikes energy sector: Symantec says a new Trojan-based campaign, focused on the Middle East, is targeting the energy industry and its trade secrets" on ZDNet. CVE is mentioned when the author states: "Symantec says the initial attack vector stems from the moneytrans[.]eu domain, which acts as an SMTP server. Emails sent from this domain contain a malicious file containing an exploit for the Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability (CVE-2012-0158). Once a victim clicks on the email and opens the attachment -- usually in the guise of an Excel file -- Laziok is dropped."

Visit CVE-2012-0158 to learn more about the issue cited above.

**CVE Mentioned in Article about Microsoft's March 2015 Patch Tuesday on NetworkWorld**

April 10, 2015

CVE is mentioned in a March 10, 2015 article entitled "March 2015 Patch Tuesday: 5 of 14 rated Critical and Microsoft issues a fix for FREAK" on NetworkWorld. CVE is mentioned when the author quotes Tripwire, Inc. security researcher Craig Young, as follows: "While Microsoft's fix to nix the FREAK attack seems to be getting all the love, "enterprises should know by now the importance of patching critical Office and Explorer vulnerabilities; MS15-027, a NETLOGON spoofing vulnerability, could be just as important to an enterprise," [Young] added. "The underlying vulnerability, CVE-2015-0005, could enable a successful attacker to move deeper into a network after breaching a workstation through a separate attack. For example an intruder could use the Office defect to gain low-level access into a network and then use impersonation techniques leveraging CVE-2015-0005 to further penetrate the network. The risk of APT and insider threat make it imperative that enterprises patch their domain controllers with MS15-027 immediately."

Visit CVE-2015-0005 to learn more about the issue cited above.

**CVE Mentioned in Article about Stuxnet on eWeek**

April 10, 2015

CVE is mentioned throughout a March 10, 2015 article entitled "Stuxnet Flaw Finally Gets Patched After More Than 4 Years" on eWeek. CVE is mentioned when the author states: "The Stuxnet worm was an exploit that was used against a nuclear facility in Iran back in 2010, in part by taking advantage of a vulnerability in Windows. The vulnerability that enabled Stuxnet was identified as CVE-2010-2568, which was thought to have been patched by Microsoft in October 2010. More than four years later, Hewlett-Packard's (HP) Zero Day Initiative (ZDI) has discovered that the CVE-2010-2568 fix was not, in fact, complete and the underlying vulnerability has remained exploitable the whole time."

CVE is mentioned a second time when the author notes that a second CVE Identifier has been issued: "The proof-of-concept code exploits that HP's ZDI provided to Microsoft on the security flaw were designed to bypass the validation checks put in place by MS10-046, the bulletin released in 2010 to patch CVE-2010-2568, [vulnerability research manager for HP Security Research Brian Gorenc said]. Rather than update the CVE-2010-2568 vulnerability information, a new identifier has been assigned with CVE 2015-0096 to encompass the expanded impact."

CVE is mentioned a third time in another quote by Gorenc, who states: "CVE-2015-0096 is a vulnerability in the Microsoft Windows operating system that allows remote attackers to execute arbitrary code by having the target simply browse to a directory containing a malicious .LNK file. The patch for CVE-2010-2568 did not completely address the issues present in the Windows Shell, and the weaknesses left are now being resolved five years later as CVE-2015-0096."

Visit CVE-2010-2568 and CVE-2015-0096 to learn more about the issues cited above.

**1 Product from ToolsWatch Now Registered as Officially "CVE-Compatible"**

March 27, 2015

One additional information security product has achieved the final stage of MITRE's formal CVE Compatibility Process and is now officially "CVE-Compatible." The product is now eligible to use the , and a completed and reviewed "CVE Compatibility Requirements Evaluation" questionnaire is posted for the product as part of the organization's listing on the CVE-Compatible Products and Services page on the CVE Web site. A total of 147 products to-date have been recognized as officially compatible.

The following product is now registered as officially "CVE-Compatible":

ToolsWatch - vFeed API and Vulnerability Database Community

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 and services 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.

**CVE Mentioned in Article about a Vulnerability in a Wind Turbine on The Register**

March 27, 2015

CVE is mentioned in a March 24, 2015 article entitled "Wind turbine blown away by control system vulnerability: Cross-site request forgery flaw takes the wind out of renewable energy" on The Register.

CVE is mentioned at the beginning of the article, when the author states: "It had to happen, we suppose: since even a utility-grade wind turbine might ship with a handy Webby control interface, someone was bound to do it badly. That's what's emerged in a new ICS-CERT advisory: CVE-2015-0985 details how turbines from US manufacturer XZERES allow the user name and password to be retrieved from the company's 442 SR turbine. As the advisory notes, "This exploit can cause a loss of power for all attached systems". The turbine in question is, according to the company, "deployed across the energy sector" worldwide."

Visit CVE-2015-0985 for more information about this issue.

**CVE Identifier "CVE-2011-2461" Cited in Numerous Security Advisories and News Media References about a Still Exploitable 4-Year-Old Adobe Flex Vulnerability**

March 27, 2015

"CVE-2011-2461" is cited in numerous major advisories, posts, and news media references related to a still exploitable four-year-old Adobe Flex vulnerability, including the following examples:

https://threatpost.com/adobe-cve-2011-2461-remains-exploitable-four-years-after-patch/111754

http://www.zdnet.com/article/patched-adobe-flex-sdk-vulnerability-remains-threat-to-web-domains/

http://www.itworld.com/article/2901235/flashbased-vulnerability-lingers-on-many-websites-three-years-later.html

http://www.theregister.co.uk/2015/03/24/borked_adobe_flash_files_expose_worlds_most_popular_sites/

http://www.cbronline.com/news/cybersecurity/data/four-year-old-flash-bug-returns-from-the-dead-4537880

http://www.computerworld.com/article/2901313/flashbased-vulnerability-lingers-on-many-websites-three-years-later.html

http://www.net-security.org/secworld.php?id=18126

http://hothardware.com/news/adobe-flex-vulnerability-that-was-patched-in-2011-still-threatens-websites

http://www.computerworld.in/news/flash-based-vulnerability-lingers-on-many-websites-three-years-later

http://www.digi.no/sikkerhet/2015/03/25/populare-nettsteder-bruker-sarbar-flash-kode

http://www.ithome.com.tw/news/94799

http://www.heise.de/security/meldung/Die-Rueckkehr-einer-totgeglaubten-Flash-Luecke-2583746.html

http://www.zdnet.fr/actualites/faille-mal-patchee-par-adobe-serieux-probleme-sur-les-videos-flash-39816848.htm

http://www.smartnews.ro/software/19043.html

http://www.zdnet.de/88229624/vor-vier-jahren-gepatchte-adobe-schwachstelle-bedroht-website-besucher/

http://japan.zdnet.com/article/35062183/

Other news articles may be found by searching on "CVE-2011-2461" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2461 includes a list of advisories used as references.

**CVE Identifiers "CVE-2015-0204" and "CVE-2015-0291" Cited in Numerous Security Advisories and News Media References about the FREAK Vulnerability**

March 20, 2015

"CVE-2015-0204" and "CVE-2015-0291" are cited in numerous major advisories, posts, and news media references related to the recent FREAK vulnerability, including the following examples:

http://www.tripwire.com/state-of-security/vulnerability-management/vert-threat-alert-openssl-vulnerability-advisory-cve-2015-0291-cve-2015-0204/

http://www.computerworld.com/article/2892926/time-to-freak-out-how-to-tell-if-youre-vulnerable.html

http://www.scmagazine.com/openssl-project-patches-two-high-severity-vulnerabilities/article/404487/

http://www.eweek.com/security/freak-attacks-ssltls-security-putting-apple-android-users-at-risk.html

http://www.scmagazine.com/freak-vulnerability-can-be-exploited-to-cause-weak-encryption/article/401691/

http://www.theregister.co.uk/2015/03/19/openssl_hello_ddod_patch_dos/

http://www.itworldcanada.com/post/another-sll-vulnerability-discovered

http://www.infosecurity-magazine.com/news/freak-show-rocks-security-industry/

http://www.scmagazineuk.com/freak-ssl-flaw-affects-mobile-browsers-thousands-of-websites/article/401539/

http://www.itproportal.com/2015/03/05/freak-flaw-intercepts-decrypts-ssl-traffic/

http://arstechnica.com/security/2015/03/openssl-warns-of-two-high-severity-bugs-but-no-heartbleed/

http://www.infoworld.com/article/2899123/security/older-openssl-versions-vulnerable-to-freak-attack.html

http://www.networkworld.com/article/2899573/openssl-fixes-serious-denialofservice-bug-11-other-flaws.html

http://www.zdnet.com/article/you-need-to-apply-the-openssl-patches-today-not-tomorrow/

https://grahamcluley.com/2015/03/freak-attack-what-is-it-heres-what-you-need-to-know/

http://news.softpedia.com/news/OpenSSL-s-Undisclosed-High-Severity-Issue-Is-Far-from-FREAK-POODLE-or-Heartbleed-476254.shtml

http://www.computerworld.com/article/2899482/openssl-fixes-serious-denial-of-service-bug-11-other-flaws.html

Other news articles may be found by searching on "CVE-2015-0204" and "CVE-2015-0291" using your preferred search engine. Also, the CVE Identifier pages https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204 and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0291 each includes a list of advisories used as references.

**CVE Editor's Commentary Blog Updated with Post about Turnaround Times on Requests for CVE IDs**

March 20, 2015

One new post has been added to the CVE-Specific section of the CVE Editor's Commentary blog in the CVE List section: "Update on Turnaround Times for CVE-Assign Requests."

The CVE Editor's Commentary blog includes opinion and commentary about CVE, vulnerabilities, software assurance, and related topics by CVE List Editor Steve Christey Coley. Posts are either Community Issues or CVE-Specific.

**CVE Included in Google's Recently Updated Vulnerability Disclosure Policy**

March 3, 2015

CVE is included in Google Inc.'s refined Vulnerability Disclosure Policy, as described in a February 13, 2015 blog post entitled "Feedback and data-driven updates to Google's disclosure policy" on its Project Zero blog. CVE is mentioned as bullet 3 of 3 as improvements to the policy, as follows: "Assignment of CVEs. CVEs are an industry standard for uniquely identifying vulnerabilities. To avoid confusion, it's important that the first public mention of a vulnerability should include a CVE. For vulnerabilities that go past deadline, we'll ensure that a CVE has been pre-assigned."

Release of the updated policy also resulted in CVE being cited in numerous major news media references and posts, including the following examples:

http://www.infosecurity-magazine.com/news/google-blinks-first-with-project/

http://www.scmagazineuk.com/under-fire-google-tweaks-bug-disclosure-policy/article/398322/

http://arstechnica.com/security/2015/02/google-updates-disclosure-policy-after-windows-os-x-zero-day-controversy/

http://www.theregister.co.uk/2015/02/14/google_vulnerability_disclosure_tweaks/

http://grahamcluley.com/2015/02/google-vulnerability-disclosure/

http://www.esecurityplanet.com/network-security/google-blinks-on-project-zero-security-disclosure.html

http://threatpost.com/google-adds-grace-period-to-disclosure-policy/111050

http://www.techtimes.com/articles/32973/20150216/google-relaxes-project-zero-90-day-deadline-other-companies-can-breathe-now.htm

Google is a CVE Numbering Authority (CNA), assigning CVE IDs for Chrome, Chrome OS, and Android Open Source Project issues. CNAs are major OS vendors, security researchers, and research organizations that assign CVE IDs newly discovered issues without directly involving MITRE in the details of the specific vulnerabilities, and include the CVE ID numbers in the first public disclosure of the vulnerabilities.

**CVE IDs Used throughout Article about "HP's Cyber Risk Report 2014" on Techworld**

March 3, 2015

CVE IDs are used throughout a February 23, 2015 article entitled "The top software exploit of 2014? The Stuxnet XP flaw from 2010, reckons HP" on TechWorld.com to uniquely identify the vulnerabilities discussed. CVE is mentioned at the very beginning of the article when the author states: "For cyber-attackers, the old flaws are still the best, according to HP's Cyber Risk Report 2014 and it has a startling piece of evidence to back up its claim – the most commonly exploited software vulnerability for last year was the infamous .lnk flaw in Windows XP made famous by Stuxnet in the distant summer of 2010. Designated CVE-2010-2568, this on its own accounted for a third of all exploits the firm detected being used against its customers, just ahead of the even older CVE-2010-0188, a flaw in Adobe's Reader and Acrobat, responsible for 11 percent of exploits." Other CVE IDs discussed in the article include CVE-2009-3129 for a Microsoft Office issue; CVE-2014-0322 and CVE-2014-0307, both for Internet Explorer issues, and CVE-2013-4787 for the Android Master Key vulnerability. An illustrated chart is also included with the article listing 10 security flaws, each of which is identified by its CVE ID number.

Visit CVE-2010-2568, CVE-2010-0188, CVE-2009-3129, CVE-2014-0322, CVE-2014-0307, CVE-2013-4787 and to learn more about the issues noted above.

**CVE IDs Used throughout Article about "HP's Cyber Risk Report 2014" on SC Magazine**

March 3, 2015

CVE is mentioned in a February 23, 2015 article entitled "Older vulnerabilities a top enabler of breaches, according to report" on SC Magazine about the "HP Cyber Risk Report 2015". CVE is mentioned at the outset of the article when the author states: "Organizations are not properly patching their systems and networks, according to the HP Cyber Risk Report 2015, which took a look back at the threat landscape in 2014 and noted that 44 percent of known breaches were possible due to vulnerabilities identified years ago. Accounting for 33 percent of identified exploit samples in 2014 is CVE-2010-2568, a popular Microsoft Windows vulnerability that was used as one of the infection vectors for Stuxnet, Jewel Timpe, senior manager of threat research at HP Security Research, told SCMagazine.com on Monday." CVE is mentioned a second time when the author states: "The report shows that CVE-2010-0188, a vulnerability in Adobe Reader and Acrobat, accounted for 11 percent of exploit samples in 2014. Six Oracle Java bugs identified in 2012 and 2013 also made the top ten list, as well as two Microsoft Office flaws – one identified in 2009 and the other in 2012."

Visit CVE-2010-2568 and CVE-2010-0188 to learn more about the issues noted above.

**CVE Mentioned in Article about Firefox Vulnerabilities on The Register**

March 3, 2015

CVE is mentioned in a February 26, 2015 article entitled "Firefox 36 swats bugs, adds HTTP2 and gets certifiably serious: Three big bads, six medium messes and 1024-bit certs all binned in one release" on The Register. CVE is mentioned when the author states: "Mozilla has outfoxed three critical and six high severity flaws in its latest round of patches for its flagship browser. It stomps out memory safety bugs, exploitable use-after-free crashes, and a buffer overflow. Of the critical crashes, bad guys could potentially craft attacks targeting MP4 video playback through a buffer overflow in the libstagefright library (CVE-2015-0829). Another potential exploitable crash that is unlikely to be a threat in email clients where scripting was disabled centres on a use-after-free flaw for specific web content with IndexedDB (CVE-2015-0831). The third are a bunch of memory bugs (CVE-2015-0836) (CVE-2015-0835) Mozilla and its fans found in the engine behind the company's products including Firefox browser that dedicated attackers could probably exploit, given enough coffee."

Visit CVE-2015-0829, CVE-2015-0831, CVE-2015-0836, and CVE-2015-0835 to learn more about these issues.

**CVE Mentioned in Article about a Samba Vulnerability on The Register**

March 3, 2015

CVE is mentioned in a February 24, 2015 article entitled "Samb-AAAHH! Scary remote execution vuln spotted in Windows-Linux interop code" on The Register. CVE is mentioned at the outset of the article when the author states: "Linux admins were sent scrambling to patch their boxes on Monday after a critical vulnerability was revealed in Samba, the open source Linux-and-Windows-compatibility software. The bug, which has been designated CVE-2015-0240, lies in the smbd file server daemon. Samba versions 3.5.0 through 4.2.0rc4 are affected, the Samba Project said in a security alert. An attacker who successfully exploits the flaw could potentially execute code remotely with root privileges, the project's developers warned. Root access is automatic and no login or authentication is necessary."

Visit CVE-2015-0240 to learn more about this issue.

**CVE Mentioned in Article about an Apple Macintosh Vulnerability on Techlicious**

March 3, 2015

CVE is mentioned in a February 18, 2015 article entitled "The Best Mac Security Software" on Techlicious. CVE is mentioned when the author states: "Many Mac owners may be under the impression that their computers don't need antivirus protection. They're inherently safer, right? While there are fewer Trojan horses, viruses and worms designed to attack Macs than PCs, that doesn't mean they're immune to infection. … In fact, a serious threat to Macs was verified as recently as December 2014, according to the National Vulnerability Database. To combat this threat, Apple issued its first ever automatic security update for Mac computers in December. (Previously, Mac users would initiate the security updates themselves.) The bug, CVE-2014-9295, could enable hackers to gain remote control of machines through a vulnerability with the network time protocol, or NTP, which synchronizes a computer's clock. It was serious enough that Apple didn't want to wait for users to fix it themselves, according to Reuters."

Visit CVE-2014-9295 to learn more about this issue.

**CVE Mentioned in Article about Android "Corrupdate" Vulnerability on Android Headlines**

March 3, 2015

CVE is mentioned in a February 18, 2015 article entitled "NowSecure Provides Fix For Serious Vulnerabilities Found In 80 Percent Of Samsung Devices Last Year" on Android Headlines. CVE is mentioned at the outset of the article, when the author states: "A major vulnerability, named "Corrupdate" because of the methods used to gain access to a pair of system applications from Samsung, has been announced; it affects nearly 80% of all Samsung Android devices including the Galaxy S5 and Note 4. The vulnerability was discovered by security researchers Ryan Welton and Jake Van Dyke of NowSecure. NowSecure, a mobile security vendor, reported the issues to Samsung and assisted with creating a patch for the affected devices. They also have confirmed that the patch that was created has appeared to work. This vulnerability affects The Samsung Account and Samsung GALAXY Applications or on some devices may be called Samsung Apps and Samsung Updates, and because they are system applications, they cannot be uninstalled. For those of you who track vulnerabilities, GALAXY Apps has been assigned CVE-2015-0863 and Samsung Account has been assigned CVE-2015-0864."

Visit CVE-2015-0863 and CVE-2015-0864 to learn more about these issues.

**CVE Mentioned in Article about Malware Research Presentations at Black Hat Asia 2015 on DarkReading.com**

March 3, 2015

CVE is mentioned in a February 26, 2015 article entitled "Black Hat Asia 2015: Target: Malware" on DarkReading.com. The main topic of the article is the upcoming Black Hat Asia 2015 conference being held on March 24- 27, 2015 in Singapore, and how "Hostile software is ever evolving, and Black Hat-associated research is one of the key loci of information on monitoring, defending against, and nullifying it. With that in mind, today we'll preview a quartet of interesting malware-related Briefings from Black Hat Asia 2015."

CVE is mentioned with regard to one of the malware-related briefings, when the author states: "The Security Content Automation Protocol (SCAP) comprises a number of open standards meant to enumerate system vulnerabilities and malware characteristics via components like Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE), and Malware Attribute Enumeration and Characterization (MAEC), which all capture high-fidelity data in XML. Unfortunately, their XML schemes lack mutual compatibility, making deeper cross-analysis difficult. Security Content Metadata Model with an Efficient Search Methodology for Real Time Monitoring and Threat Intelligence proposes a low-impact way to modify these schema which will result in more powerful analyses that can resolve vulnerabilities before they're exploited."

**2nd Product from Beijing Netpower Technologies Now Registered as Officially "CVE-Compatible"**

February 12, 2015

One additional information security product has achieved the final stage of MITRE's formal CVE Compatibility Process and is now officially "CVE-Compatible." The product is now eligible to use the , and a completed and reviewed "CVE Compatibility Requirements Evaluation" questionnaire is posted for the product as part of the organization's listing on the CVE-Compatible Products and Services page on the CVE Web site. A total of 146 products to-date have been recognized as officially compatible.

The following product is now registered as officially "CVE-Compatible":

Beijing Netpower Technologies Inc. - Netpower Network Intrusion Detection System

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 and services 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.

**ToolsWatch Makes Declaration of CVE Compatibility**

February 12, 2015

ToolsWatch declared that its open source correlated and cross-linked vulnerability XML vulnerability database, vFeed API and Vulnerability Database Community, is CVE-Compatible. For additional information about this and other CVE-Compatible products, visit the CVE-Compatible Products and Services section.

CVE Identifier "CVE-2015-0313" Cited in Numerous Security Advisories and News Media References about a Zero-Day Adobe Flash Vulnerability

February 12, 2015

"CVE-2015-0313" was cited in numerous major advisories, posts, and news media references related to the recent zero-day Adobe Flash vulnerability, including the following examples:

http://www.computerworld.com/article/2879997/adobe-rolls-out-patches-for-latest-flash-flaw.html

http://www.eweek.com/security/new-zero-day-exploit-adds-to-adobe-flash-security-woes.html

http://www.theregister.co.uk/2015/02/02/flash_0day_patch_not_another_one/

http://www.scmagazine.com/adobe-warns-flash-users-of-zero-day-vulnerability/article/395957/

http://www.cio-today.com/article/index.php?story_id=0030003H7793

http://www.computerworld.com/article/2877986/flash-player-faces-its-third-zero-day-flaw-in-a-month-updates-coming.html

http://arstechnica.com/security/2015/02/as-flash-0day-exploits-reach-new-level-of-meanness-what-are-users-to-do/

http://gadgets.ndtv.com/internet/news/adobe-says-fix-for-latest-flash-player-zero-day-vulnerability-due-soon-656802

http://grahamcluley.com/2015/02/adobe-flash-zero-day-vulnerability-exploited-hackers-infect-ie-firefox-users/

http://threatpost.com/latest-flash-0day-under-attack-possible-ties-to-group-behind-angler-ek/110847

https://www.virusbtn.com/blog/2015/02_05.xml

http://www.cso.com.au/article/565327/adobe-patches-another-0-day-flash-used-infect-dailymotion-visitors/

http://www.technewsworld.com/story/81678.html

http://www.itworld.com/article/2880295/adobe-starts-patching-latest-flash-flaw.html

http://www.itpro.co.uk/security/23978/adobe-releases-third-unscheduled-flash-security-update

https://hacked.com/yet-another-adobe-flash-zero-day-vulnerability/

http://www.darkreading.com/new-adobe-flash-0-day-used-in-malvertising-campaign/d/d-id/1318900

http://www.jbgnews.com/2015/02/third-flaw-exploited-for-adobe-flash-player-in-a-month/463906.html

http://www.businesswire.com/news/home/20150202006158/en/Trend-Micro-Alerts-U.S.-Market-Adobe-Flash

http://www.theinquirer.net/inquirer/news/2393383/adobe-flash-zero-day-flaw-exploited-again

http://betanews.com/2015/02/02/surprise-adobe-flash-has-a-security-flaw-on-windows-mac-and-linux/

http://techreport.com/news/27777/flash-has-already-suffered-three-zero-day-exploits-in-2015

http://www.net-security.org/malware_news.php?id=2955

http://www.techweekeurope.co.uk/security/virus/adobe-release-security-patches-160785

http://www.gadget.co.za/pebble.asp?relid=9459

http://mybroadband.co.za/news/security/118255-adobe-flash-zero-day-exploit.html

http://www.infosecurity-magazine.com/news/flash-zeroday-dailymotioncom-for/

Other news articles may be found by searching on "CVE-2015-0313" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0313 includes a list of advisories used as references.

**1 Product from WPScan Now Registered as Officially "CVE-Compatible"**

February 4, 2015

One additional information security product has achieved the final stage of MITRE's formal CVE Compatibility Process and is now officially "CVE-Compatible." The product is now eligible to use the , and a completed and reviewed "CVE Compatibility Requirements Evaluation" questionnaire is posted for the product as part of the organization's listing on the CVE-Compatible Products and Services page on the CVE Web site. A total of 145 products to-date have been recognized as officially compatible.

The following product is now registered as officially "CVE-Compatible":

WPScan - WPScan Vulnerability Database

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 and services 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.

**1 Product from Beijing Netpower Technologies Now Registered as Officially "CVE-Compatible"**

February 4, 2015

One additional information security product has achieved the final stage of MITRE's formal CVE Compatibility Process and is now officially "CVE-Compatible." The product is now eligible to use the , and a completed and reviewed "CVE Compatibility Requirements Evaluation" questionnaire is posted for the product as part of the organization's listing on the CVE-Compatible Products and Services page on the CVE Web site. A total of 145 products to-date have been recognized as officially compatible.

The following product is now registered as officially "CVE-Compatible":

Beijing Netpower Technologies Inc. - Netpower Network Vulnerability Scanner

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 and services 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.

**CVE Identifier "CVE-2015-0235" Cited in Numerous Security Advisories and News Media References about "Ghost" Vulnerability**

January 30, 2015

"CVE-2015-0235" was cited in numerous major advisories, posts, and news media references related to the recent Ghost vulnerability, including the following examples:

http://www.scmagazine.com/buffer-overflow-vulnerability-in-linux-identified/article/395025/

http://www.darkreading.com/vulnerabilities---threats/new-ghost-vuln-affecting-linux/d/d-id/1318811

http://www.infosecurity-magazine.com/news/admins-urged-to-patch-linux-ghost/

http://www.theregister.co.uk/2015/01/28/ghost_linux_megavuln_analysis/

http://www.zdnet.com/article/critical-linux-security-hole-found/

http://arstechnica.com/security/2015/01/highly-critical-ghost-allowing-code-execution-affects-most-linux-systems/

http://threatpost.com/ghost-glibc-remote-code-execution-vulnerability-affects-all-linux-systems/110679

http://www.itworld.com/article/2876098/linux-hit-by-critical-security-hole.html

http://www.tomsguide.com/us/ghost-linux-flaw,news-20366.html

http://www.techworm.net/2015/01/ghost-vulnerability-in-gnu-c-library-can-be-exploited-remotely-to-hijack-the-linux.html

http://www.slashgear.com/linux-c-library-exploit-affects-all-systems-dating-back-2000-28366406/

http://www.net-security.org/secworld.php?id=17886

http://www.theinquirer.net/inquirer/news/2392473/ghost-in-the-linux-machine-hits-debian-red-hat-and-ubuntu

http://betanews.com/2015/01/27/warning-linux-is-being-haunted-by-a-g-g-g-ghost-vulnerability-are-you-at-risk/

http://searchsecurity.techtarget.com/news/2240238974/Qualys-finds-GHOST-Critical-Linux-remote-code-execution-flaw

http://www.v3.co.uk/v3-uk/news/2392369/ghost-linux-bug-haunting-red-hat-and-ubuntu-systems

http://www.techweekeurope.co.uk/software/open-source/severe-linux-ghost-flaw-spooks-computer-users-160396

http://www.cso.com.au/article/564898/remotely-exploitable-ghost-bug-strikes-all-linux-distros/

http://www.journaldunet.com/solutions/saas-logiciel/une-nouvelle-faille-critique-ghost-rend-les-systemes-linux-vulnerables-0115.shtml

http://www.searchsecurity.de/news/2240238996/Security-Ticker-Antivirus-App-als-Scareware-GHOST-Luecke-in-Linux-IBM-Identity-Mixer

http://www.itespresso.fr/securite-it-ghost-plane-linux-86944.html

http://www.silicon.de/41608362/sicherheitsleck-ghost-bedroht-linux-systeme/

http://www.theregister.co.uk/2015/01/27/glibc_ghost_vulnerability/

https://nakedsecurity.sophos.com/2015/01/29/the-ghost-vulnerability-what-you-need-to-know/

http://www.eweek.com/security/ghost-bug-not-new-but-can-haunt-older-linux-versions.html

http://www.itproportal.com/2015/01/29/deal-linux-ghost-vulnerability/

Other news articles may be found by searching on "CVE-2015-0235" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235 includes a list of advisories used as references.

**CVE Mentioned in Article about Disclosing and Patching Vulnerabilities on Tripwire's State of Security Blog**

January 30, 2015

CVE is mentioned in a January 20, 2014 article about responsible vulnerability disclosure entitled "Hacker halted… What is it?" on the Tripwire, Inc.'s State of Security blog. The article is a follow-up to a presentation by Tripwire's Vulnerability and Exposures Research Team at "Hacker Halted 2014" about the vulnerability disclosure process and the turnaround times for creating patches.

CVE is mentioned in a section of the article entitled "Responsible Disclosure," when the author states:

"There are a few steps to properly disclose a vulnerability to a vendor.

1. Determine if the vendor is a CVE Numbering Authority (CNA). If they are ([MITRE] maintains a list at: https://cve.mitre.org/cve/cna.html), you can contact the vendor directly. If they aren't, you can request a CVE from [MITRE].
2. Determine the vendor security contact.
3. Send all relevant information to the contact.
4. You now have to follow up with the vendor until the issue has been resolved. Once resolved and a patch has been released you can release your information about the vulnerability to the public."

The author concludes the article as follows: "If we don't properly disclose vulnerabilities, we not only hurt ourselves but we hurt others. It's like driving home drunk — the moment you get into your vehicle you put your life, and others, at risk. While a vulnerability may not be as dire, we need to work together with the vendors to properly disclose and fix vulnerabilities."

**First CVE IDs Issued in New Numbering Format Now Available**

January 13, 2015

The first ever CVE ID numbers issued in the new CVE ID numbering format were posted on January 13, 2015 for vulnerabilities disclosed in 2014: CVE-2014-10001 with 5 digits and CVE-2014-100001 with 6 digits.

The format of CVE ID numbers was changed a year ago this month in January 2014 so that the CVE project can track 10,000 or more vulnerabilities for a given calendar year. Previously, CVE IDs were restricted to four digits at the end in the sequence number portion of the ID, for example "CVE-2014-0160", but this four-digit restriction only allowed up to 9,999 vulnerabilities per year. With the new format, CVE ID numbers may have 4, 5, 6, 7, or more digits in the sequence number if needed in a calendar year. For example, the just released "CVE-2014-10001" with 5 digits in the sequence number and "CVE-2014-100001" with 6 digits in the sequence number, or CVE-2014-XXXXXXX with 7 digits in the sequence number, and so on.

Additional CVE IDs in the new format with 5 and 6 digits in the sequence number were also issued today—CVE-2014-10001 through CVE-2014-10039 with 5 digits, and CVE-2014-100001 through CVE-2014-100038 with 6 digits—to also identify vulnerabilities disclosed in 2014. Enter these CVE ID numbers on the CVE List search page to learn more about each issue.

Please report any problems, or anticipated problems, that you encounter with CVE IDs issued in the new format to cve-id-change@mitre.org.

**CVE Editor's Commentary Page Updated**

January 13, 2015

One new item has been added to the CVE-Specific section of the CVE Editor's Commentary page in the CVE List section: "CVE IDs Posted Today for the First Time Using the New ID Syntax."

The CVE Editor's Commentary page includes opinion and commentary about CVE, vulnerabilities, software assurance, and related topics by CVE List Editor Steve Christey. Posts are either Community Issues or CVE-Specific.

**CVE Mentioned in Article about Vulnerabilities in Software Libraries on TechWorld.com**

January 8, 2015

CVE is mentioned in a January 5, 2015 article entitled "Think that software library is safe to use? Think again…" on TechWorld.com. The main topic of the article is that third-party software code libraries and components are not bug-free and that the "major patching efforts triggered by the Heartbleed, Shellshock and POODLE flaws last year highlight the effect of critical vulnerabilities in third-party code. The flaws affected software that runs on servers, desktop computers, mobile devices and hardware appliances, affecting millions of consumers and businesses."

CVE is first referenced as an example when the author states: "One example… is a vulnerability discovered in 2006… The flaw was among several that affected LibTIFF and were fixed in a new release at the time. It was tracked as CVE-2006-3459 in the Common Vulnerabilities and Exposures database." CVE is mentioned again in a quote about this example by Risk Based Security, Inc.'s Chief Research Officer, Carsten Eiram, who states: "In 2010, a vulnerability was fixed in Adobe Reader, which turned out to be one of the vulnerabilities covered by CVE-2006-3459. For four years, a vulnerable and outdated version of LibTIFF had been bundled with Adobe Reader, and it was even proven to be exploitable. Adobe Systems has since become one of the software vendors taking the threat of flaws in third-party components seriously. They've made major improvements to their process of tracking and addressing vulnerabilities in the third-party libraries and components used in their products."

Visit CVE-2006-3459 to learn more about the issue cited above. To learn about "Heartbleed" see CVE-2014-0160; for "Bash Shellshock" see CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, and CVE-2014-6278; and for "POODLE" see CVE-2014-3566.

**CVE Identifier "CVE-2014-9295" Cited in Numerous Security Advisories and News Media References about the Apple/Linux Network Time Protocol Vulnerability**

January 8, 2015

"CVE-2014-9295" was cited in numerous major advisories, posts, and news media references related to the recent Network Time Protocol vulnerability affecting Apple and Linux operating systems, including the following examples:

http://www.infoworld.com/article/2862197/networking/exploits-for-dangerous-network-time-protocol-vulnerabilities-can-compromise-systems.html

http://www.forbes.com/sites/amitchowdhry/2014/12/26/why-apple-pushed-its-first-automatic-mac-os-x-security-update-this-week/

http://www.cnet.com/news/apple-updates-macs-without-asking-but-its-to-foil-hackers/

http://www.cbronline.com/news/security/apple-rolls-out-first-ever-automated-security-update-241214-4477252

http://www.v3.co.uk/v3-uk/news/2388048/apple-issues-first-automatic-os-x-security-update

http://www.franchiseherald.com/articles/18506/20141223/apple-mac-os-update.htm

http://www.breathecast.com/articles/apple-new-mac-os-x-update-automatic-patch-combats-hacker-22904/

http://www.theinquirer.net/inquirer/news/2388059/apple-os-x-users-at-risk-from-critical-security-issue

http://en.kioskea.net/news/25695-apple-pushing-mac-update-automatically

http://zolmax.com/business/apple-releases-first-ever-automated-security-update/272439/

http://www.itespresso.fr/securite-it-os-x-apple-automatique-85633.html

http://www.pianetacellulare.it/Articoli/Apple/36639_Apple-aggiorna-Mac-in-automatico-senza-chiedere-agli-utenti.php

http://www.chinatopix.com/articles/29342/20141224/apple-pushes-first-automatic-update-mac-os-x.htm

http://www.networkworld.com/article/2862233/exploits-for-dangerous-network-time-protocol-vulnerabilities-can-compromise-systems.html

http://www.tomsguide.com/us/apple-ntp-patch,news-20057.html

http://www.valuewalk.com/2014/12/apple-just-gave-security-update-didnt-ask-first/

http://www.emirates247.com/business/technology/hackers-target-mac-machines-apple-hits-back-2014-12-24-1.574393

http://www.computerworld.com/article/2862138/exploits-for-dangerous-network-time-protocol-vulnerabilities-can-compromise-systems.html

Other news articles may be found by searching on "CVE-2014-9295" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9295 includes a list of advisories used as references.

**CVE Identifier "CVE-2014-9222" Cited in Numerous Security Advisories and News Media References about "Misfortune Cookie" Vulnerability**

January 8, 2015

"CVE-2014-9222" was cited in numerous major advisories, posts, and news media references related to the recent Misfortune Cookie vulnerability, including the following examples:

http://www.techworld.com/news/security/dangerous-misfortune-cookie-flaw-discovered-in-12-million-home-routers-3591547/

http://www.theregister.co.uk/2014/12/18/misfortune_cookie/

http://www.cio.com/article/2861233/vulnerability-in-embedded-web-server-exposes-millions-of-routers-to-hacking.html

http://arstechnica.com/security/2014/12/12-million-home-and-business-routers-vulnerable-to-critical-hijacking-hack/

http://www.scmagazine.com/crucial-vulnerability-could-compromise-at-least-200-router-models/article/389149/

http://www.scmagazineuk.com/millions-of-routers-and-pcs-vulnerable-to-decade-old-cookie-flaw/article/389031/

http://www.cso.com.au/article/562848/check-point-researchers-discover-significant-vulnerability-could-used-take-control-millions-consumer-business-internet-routers/

http://www.cso.com.au/article/562848/check-point-researchers-discover-significant-vulnerability-could-used-take-control-millions-consumer-business-internet-routers/

http://www.marketwatch.com/story/media-alert-check-point-researchers-discover-significant-vulnerability-that-could-be-used-to-take-control-of-millions-of-consumer-and-business-internet-routers-2014-12-18

http://www.evdoinfo.com/content/view/4966/64/

http://www.infosecurity-magazine.com/news/critical-flaw-hits-millions-of/

http://www.securityweek.com/misfortune-cookie-vulnerability-exposes-millions-routers

http://thehackernews.com/2014/12/router-vulnerability-puts-12-million.html

http://www.pcworld.com/article/2861232/vulnerability-in-embedded-web-server-exposes-millions-of-routers-to-hacking.html

http://www.techworm.net/2014/12/12-million-officehome-routers-vulnerable-misfortune-cookie-attacks.html

Other news articles may be found by searching on "CVE-2014-9222" using your preferred search engine. Also, the CVE Identifier page https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9222 includes a list of advisories used as references.

**CVE Identifier "CVE-2014-9390" Cited in an Article about a Git Source Code Management System Vulnerability on eWeek**

January 8, 2015

"CVE-2014-9390" was cited in a December 20, 2014 article entitled "Git Vulnerability Exposed; Patch Now or Be Hacked Later" on eWeek.com. CVE is mentioned at the beginning of the article when the author states: "A new vulnerability has been reported and was patched on Dec. 18 in the widely used open-source Git source-code management system. The vulnerability has been identified as CVE-2014-9390 and impacts Git clients running on Windows and Mac OS X. Git is an open-source source-code management system used by developers on Linux, Windows and Mac OS X, and includes both a host server-side component as well as a local client on developer machines. Git is also the open-source technology behind the popular GitHub code repository. Linus Torvalds, best known as the creator of the open-source Linux operating system, developed Git. Somewhat ironically, the author of the rival Mercurial open-source version control system first discovered the CVE-2014-9390 issue, which also impacts Mercurial."

CVE is mentioned again when the author notes that patches are now available for the issue: "The fix for the CVE-2014-9390 vulnerability is now present in the new Git v2.2.1 release and has also been patched in Mercurial version 3.2.3. Although the issue only directly affects Windows and Mac OS X users, Linux users are also being advised to be cautious." CVE is mentioned for a third time at the end of the article, as follows: "Metasploit is often the first place where new exploits come for security researchers to be able to test vulnerabilities. It is likely that an exploit for CVE-2014-9390 will find its way into Metasploit at some point to be able to demonstrate the vulnerability."

Visit CVE-2014-9390 to learn more about this issue.