Counterintelligence Working Group NEW MEXICO

NMCIWG Purple Arrow

The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
28 April 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, Sandia Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings Credit is given to the NMCIWG for the compilation of open source data

Security flaw puts all Internet Explorer users at risk, exposes Windows XP

The Verge, 27 Apr 2014: If you're still using a 12-year-old operating system, a new security flaw discovered in Internet Explorer should cause you quite a bit of consternation. Microsoft published a security advisory today warning its customers that a vulnerability in all versions of Internet Explorer (6 through 11) could let hackers gain full user permissions over your computer, allowing them to install programs, view and delete data, and much more simply by visiting a website. That's not good, but at least anyone using Internet Explorer on a modern version of Windows will likely see a patch within a couple weeks' time. Since Microsoft finally ended support for Windows XP on April 8th, it will not receive an update. This is the first known security flaw since that support deadline passed, and it bears true the warnings voiced by the tech community. Windows XP is no longer secure, and it's time to move on. To read more click **HERE**

Microsoft rushes to fix browser after attacks; no fix for XP users

Reuters, 27 Apr 2014: Microsoft Corp is rushing to fix a bug in its widely used Internet Explorer web browser after a computer security firm disclosed the flaw over the weekend, saying hackers have already exploited it in attacks on some U.S. companies. PCs running Windows XP will not receive any updates fixing that bug when they are released, however, because Microsoft stopped supporting the 13-year-old operating system earlier this month. Security firms estimate that between 15 and 25 percent of the world's PCs still run Windows XP. Microsoft disclosed on Saturday its plans to fix the bug in an advisory to its customers posted on its security website, which it said is present in Internet Explorer versions 6 to 11. Those versions dominate desktop browsing, accounting for 55 percent of the PC browser market, according to tech research firm NetMarketShare. Cybersecurity software maker FireEye Inc said that a sophisticated group of hackers have been exploiting the bug in a campaign dubbed "Operation Clandestine Fox." FireEye, whose Mandiant division helps companies respond to cyber attacks, declined to name specific victims or identify the group of hackers, saying that an investigation into the matter is still active. "It's a campaign of targeted attacks seemingly against U.S.-based firms, currently tied to defense and financial sectors," FireEye spokesman Vitor De Souza said via email. "It's unclear what the motives of this attack group are, at this point. It appears to be broad-spectrum intel gathering." Microsoft said in the advisory that the vulnerability could allow a hacker to take complete control of an affected system, then do things such as viewing changing, or deleting data, installing malicious programs, or creating accounts that would give hackers full user rights. FireEye and Microsoft have not provided much information about the security flaw or the approach that hackers could use to figure out how to exploit it, said Aviv Raff, chief technology officer of cybersecurity firm Seculert. Yet other groups of hackers are now racing to learn more about it so they can launch similar attacks before Microsoft prepares a security update, Raff said. "Microsoft should move fast," he said. "This will snowball." Still, he cautioned that Windows XP users will not benefit from that update since Microsoft has just halted support for that product. The software maker said in a statement to Reuters that it advises Windows XP users to upgrade to one of two most recently versions of its operating system, Windows 7 or 8. To read more click **HERE**

ArticleRPT-U.S. Homeland Security struggles to tempt, retain cyber talent

Reuters, 28 Apr 2014: In the race to attract cybersecurity experts to protect the government's computer networks, the Department of Homeland Security has a handicap money can't fix. Navigating the federal hiring system takes many months, which is too long in the fast-paced tech world. "Even when somebody is patriotic and wants to do their duty for the nation, if they're really good they're not going to wait six months to get hired," said Mark Weatherford, the former cyber chief at DHS. After a spate of national security leaks and with cybercrime on the rise, the department is vying with the private sector and other three-letter federal agencies to hire and retain talent to secure federal networks and contain threats to American businesses and utilities. Phyllis Schneck, the former chief technology officer at security software company McAfee Inc who succeeded Weatherford in August, asked a U.S. Senate committee for help. "The hiring process is very, very difficult," she said. Cyber experts can command higher salaries - in some cases up to six figures more - at private companies, Schneck said, but national security offers a "higher calling" and valuable experience. "People say the good talent doesn't come because we can't pay them," she said. "We could actually use our mission to outdo some of those salaries they're offered. But we have to have the flexibility and some additional competitiveness to bring them inside." The Homeland Security Department, created after the Sept. 11, 2001, attacks, is playing catchup with the Pentagon's larger and more established cybersecurity operations at Cyber Command and the National Security Agency. Not only does DHS lack the enhanced hiring powers of its military counterpart and the agility private companies offer, but the rigid bureaucracy of the 240,000-employee agency can foster an inside-the-box culture. "There's a lot of really smart, scary cybersecurity professionals out there who also happen to have pink hair and tattoos," said Weatherford. But you won't find them at DHS, which also is averse to hiring cyber experts without a college degree, he said. "Some of the smartest and most talented people I know in this business don't have a degree," said Weatherford, who left the agency a year ago for the Chertoff Group consulting firm, founded by a previous DHS secretary, Michael Chertoff. DHS Secretary Jeh Johnson, who took office in December, has promised to get personally involved in recruiting and make "new hiring and pay flexibility to recruit cybersecurity talent" a legislative goal. Specifically, DHS wants the secretary to be able to make direct appointments and reform job descriptions and requirements for certain cybersecurity positions, and to set salaries and offer additional incentives, a department official said At a Senate Homeland Security and Governmental Affairs Committee hearing on March 26, ranking Republican Senator Tom Coburn assured Schneck, "we're going to get you the capability to hire the people you need." Coburn and Democratic Chairman Thomas Carper are working on a measure to help DHS boost its cyber workforce by giving it the same hiring and compensation powers as the Defense Department, a committee aide said. The federal government follows a strict hiring protocol that includes a long application, background check and in some cases a security clearance. It can take from a few months to more than a year, said Max Stier, president of the nonprofit Partnership for Public Service. The onerousness of the process is "true for cyber, and it's true for every mission-critical occupation that the government has," he said. Nevertheless, the problem is especially acute in a fast-moving, well-compensated field like cybersecurity, where the qualified can write their own tickets. The mission could scarcely be more critical. Security lapses at government agencies can lead to such diplomatic and national security crises as the fallout from revelations of former NSA contractor Edward Snowden and WikiLeaks' release of State Department cables obtained by U.S. soldier Bradley Manning. A recent RAND Corp study found that "the ability to stage cyberattacks will likely outpace the ability to defend against them" and that cybercrime can be more lucrative than the illegal drug trade. Experts say Homeland Security doesn't have to wait for legislation. "It's self-inflicted damage, it's not that they need something from Congress," said Alan Paller, co-chairman of a task force DHS set up two years ago to recommend ways DHS could improve its cyber force. DHS can bypass time-consuming security clearances and fight cyber attacks more efficiently by declassifying work that is not secret, said Amit Yoran, a senior vice president at security company RSA who held top DHS posts in the George W. Bush administration. He warned lawmakers about the hiring problems in 2009. "I called this out as a key issue or critical issue, which I don't think is solved," he said. The department works daily with companies and utilities to secure computer networks for water systems, the electric grid, financial, commercial, agriculture and healthcare services. Weatherford said that work was "99.99 percent unclassified," but since it was performed in a classified DHS facility, it had to be labeled secret. Also, the agency still tends to award outside contractors the most coveted cyber jobs, including those for forensics investigators and intrusion malware and detection engineers who understand how attacks work, said Paller. "The good technical people want to go to work where they will grow," Paller said. "It's especially true in this field because the bad guys are changing the game all the time." In the fall of 2012, the task force recommended hiring cyber experts with advanced technical skills as part of a specialist corps with enticing missions and growth potential. DHS spokesman S.Y. Lee said the department offers strong cybersecurity career paths, including scholarship, fellowship and internship programs to attract and keep top talent. The task force recommended DHS have 600 federal workers in cybersecurity positions that have certain mission-critical skills. DHS then did a review and identified 1,500 such positions. But Paller, founder of SANS professional cybersecurity training institute, said very few of the people in them have the advanced technical skills needed to carry out DHS' mission of protecting the federal government's computers. "Right now, I don't think they can," he said. DHS has fended off calls over the years, including from Republican Senator John McCain, to transfer its cyber operations to the larger and better-resourced Pentagon, which aims to have a 6,000-member cyber force by 2016. To read more click **HERE**

Ditch Internet Explorer on XP, security experts warn
Theguardian.com, 28 April 2014: Security experts have urged Windows XP users to change browsers owing to a serious bug in Microsoft's Internet Explorer that could threaten over half of all internet users. The vulnerability is actively being exploited by hackers, Microsoft has warned, and every active version of Internet Explorer is at risk, including IE 6 to IE 11, Windows XP and Windows RT. The bug could allow hackers to gain access to and hijack a Windows computer, including personal data. Microsoft warned that it was "aware of limited, targeted attacks" currently under way using the security hole in Internet Explorer, which is used by over 55% of internet users globally, according to the latest data from research firm Netmarketshare. "This issue allows remote code execution if users visit a malicious website with an affected browser. This would typically occur by an attacker convincing someone to click a link in an email or instant message," Dustin Childs, a group manager of Microsoft's Trustworthy Computing department, explained in a blog post. Microsoft issued security advice over the weekend, saying it was investigating the flaw and will take "appropriate action to protect our customers", including patching the security hole, originally found by security company FireEye. The flaw affects users of Internet Explorer on multiple Windows software versions, including Windows Vista, 7 and the latest Windows 8. But the biggest threat is posed to the 13-year-old Windows XP, which Microsoft recently withdrew support for and is still used on an estimated 430m computers globally. It is unknown whether Microsoft will backtrack on its support withdrawal to fix the security hole in Internet Explorer on Windows XP. Microsoft's security note explained that hackers looking to take advantage of the bug to take complete control of a user's computer via Internet Explorer would require users to view a "specially crafted website". Microsoft advised users to be careful about clicking on suspicious links that could take them to the hacker's site when browsing, emailing or chatting via instant messenger. The company also explained a series of work arounds that could help protect users, which include installing a Microsoft tool kit that enhances the security of Internet Explorer. "We encourage customers to follow the suggested mitigations outlined in the security advisory while an update is finalised," a Microsoft spokesperson told the Guardian. To read more click **HERE**

April 25, Softpedia – (International) **Nine members of cybercrime ring sentenced to a total of 24 years for attacks on banks.** Nine men found guilty of stealing around $2.1 million from Barclays and Santander banks were sentenced by a U.K. court to serve a total of 24 years and 9 months. The group used keyboard, video, mouse (KVM) switches to transfer money from the banks, and also intercepted around one million letters to obtain payment cards that were then used to make fraudulent purchases. Source: http://news.softpedia.com/news/Nine-Members-of-Cybercrime-Ring-Sentenced-to-a-Total-of-24-Years-for-Attacks-on-Banks-439394.shtml

April 24, Boston Globe – (Massachusetts) **Social security numbers stolen from Tufts Health members.** Tufts Health Plan notified about 8,830 former and current insurance plan holders that their personal data, including their Social Security numbers, were stolen. The health insurer reported the theft was not due to an electronic breach or IT system hacking. Source: http://www.bostonglobe.com/business/2014/04/24/personal-information-stolen-from-more-than-members-tufts-health-plan/jAwJkp4WQDCWPwQYCNNquM/story.html

April 23, Stroudsburg Pocono Record – (Pennsylvania) **Patient information may have been on stolen Coordinated Health laptop.** Coordinated Health announced April 23 that a password-protected laptop that may contain the personal information of 733 patients was stolen from an employee's car in Bethlehem February 21 and has not been recovered. Hospital officials are working with authorities to investigate the incident. Source: http://www.poconorecord.com/apps/pbcs.dll/article?AID=/20140423/NEWS/140429901

April 25, Softpedia – (International) **Heartbleed bug patched on all US government websites.** Trend Micro researchers reported that less than 10 percent of Web sites remain vulnerable to the Heartbleed flaw in OpenSSL, with all U.S. government Web sites patched. Distil Networks researchers also reported that 84 percent of the top 10,000 global Web sites have applied patches to close the vulnerability. Source: http://news.softpedia.com/news/Heartbleed-Bug-patched-on-All-US-Government-Websites-439271.shtml

April 24, Threatpost – (International) **Apache warns of faulty zero day patch for Struts.** The Apache Software Foundation (ASF) released an advisory April 24 stating that a patch issued in March to close a zero day vulnerability in Apache Struts did not completely close the vulnerability. The advisory stated that a new patch would likely be released within 72 hours, and ASF provided a temporary mitigation for users to apply until then. Source: http://threatpost.com/apache-warns-of-faulty-zero-day-patch-for-struts/105691

April 24, SC Magazine – (International) **No encryption means easy compromise of Viber location data, communications.** Researchers with the University of New Haven Cyber Forensics Research & Education Group reported that the Viber text message and voice over IP (VoIP) service manages data in an unencrypted form that could allow attackers and service providers to intercept data being sent and stored. Source: http://www.scmagazine.com/no-encryption-means-easy-compromise-of-viber-location-data-communications/article/344109/

Organized Crime Group Scams US Companies Out Of Millions

DarkReading, 28 Apr 2014: Social engineering attack tricks companies into large wire transfers.An organized crime group has spent the last month defrauding US companies, fooling them into making large wire transfers into fake partners' accounts. According to a blog posted Friday by researchers at security firm TrustedSec, the crime group is conducting "a major offensive" against US firms using a sophisticated social engineering attack that appears to be a request for funds from one of the victim companies' legitimate partners. The attacks have a high rate of success, often fooling enterprises into sending amounts of $50,000 to $1 million, the blog says. "A number of companies are still unaware that they have been victims of this attack," TrustedSec says. The attack works in much the same way as a traditional phishing attack, only the stakes are much higher. The attacker compromises an email account in the victim's accounting department -- or that of the business partner -- and then registers an Internet domain that is very similar to the partner's legitimate domain name. The attacker will establish communications with the victim using the partner's email credentials, often communicating via legitimate company letterhead with legitimate signatures. Initially, the communications may include the legitimate domain names. Once communications have been established, the attacker will then submit requests for funds, change orders, or lines of credit from the victim company, TrustedSec says. If the initial requests don't work, the attacker may spoof emails to authorize the funds transfer or conduct a convincing social engineering attack over the phone. The attackers often are successful in getting wire transfers to the fake domains, the blog says. A large number of the transfers are processed by banks in China. "Note that the attackers are persistent; they use emotional triggers in order to entice the affected company to expedite the fraudulent requests," says TrustedSec. "They will become agitated, demand that it be expedited and even spoof emails coming from internal employees to coax the company to hurrying the process. They will also target your company again if successful." IT organizations should warn their accounting departments about this fraud and verify all transactions with third-party partners and vendors, TrustedSec advices. To read more click **HERE**

Security Researchers Warn Military Satellites Could Be Hacked

The Christian Science Monitor, 25 Apr 2014 Satellite communication terminals, relied upon by US military aircraft, ships, and land vehicles to move in harmony with one another, are susceptible to cyber-attack through digital backdoors and other vulnerabilities, according to a new report that has sent a tremor through the global satellite telecommunications industry. The report by IOActive, a Seattle-based cyber-security firm, arrives amid heightened concerns over a surge in cyber-attacks against satellite communications systems and vendors worldwide, industry experts say. According to the IOActive report, a forensic security analysis of computer code buried inside the circuit boards and chips of the world’s most widely used SATCOM terminals found multiple potential hacker entry points. Many terminals use small dishes or receivers that ride on the roof of a military vehicle, the bridge of a ship, or inside a troop transport aircraft, the report said. Built by a half-dozen of the world’s leading SATCOM equipment manufacturers, the SATCOM terminals cited in the report also serve nonmilitary uses, such as data collection from remote oil and gas pumping sites, pipelines, or retail chain stores. All involve sending data from far-flung operations up to large commercial satellite networks and back down again to their respective headquarters. Industry officials, who generally acknowledged the proliferation of cyber-threats to the communications industry and were aware of the IOActive report, say SATCOM terminals are very secure when security features are turned on and used properly and are not insecure by design. But what cyber-security researchers found when reverse-engineering the SATCOM terminals’ firmware – the core computer code stored on the memory chips that primarily control the equipment – was a shocker, they said. “IOActive found that malicious actors could abuse all of the devices within the scope of this study,” wrote report author Ruben Santamarta, a principal consultant to the company. “These vulnerabilities have the potential to allow a malicious actor to intercept, manipulate, or block communications, and in some cases, to remotely take control of the physical device.” Vulnerabilities in the firmware include digital “backdoors” built into the computer code, as well as “hardcoded credentials,” either of which could be used for unauthorized easy access to the devices, according to the report. In addition, insecure communications protocols (languages) and relatively weak encryption on the system were other key problems, said the report, titled “A Wake-up Call for SATCOM Security.” In at least some cases, an adversary might need only send a text message that included malicious code – one of several options – to take control of the SATCOM terminal, the researchers said. A nation-state adversary or hacker could then fake the locations of aircraft, ships, and ground forces – as well as emergency messages. “If one of these affected devices can be compromised, the entire SATCOM infrastructure could be at risk,” the report says. “Ships, aircraft, military personnel, emergency services, media services, and industrial facilities (oil rigs, gas pipelines, water treatment plants, wind turbines, substations, etc.) could all be impacted by the vulnerabilities.” “The findings,” Mr. Santamarta noted, “should serve as an initial wake-up call for both the vendors and users” of current SATCOM technology. If the US military is concerned that SATCOM systems may be vulnerable to cyber-attack, it’s hard to tell. “The Department of Defense is aware of a multitude of growing threats in cyber-space, that anything connected to the Internet is potentially vulnerable,” Lt. Col. Valerie D. Henderson, a Department of Defense spokeswoman, said Thursday in a statement responding to Monitor queries. “We manage all cyber-risks in accordance with one of DoD's primary cyber-space missions: Defense of all DoD information networks. We do not comment on specific operational vulnerabilities or the actions that we take to manage the associated risks, in order to preserve our operational security.” Other experts note that it’s often easier to identify a vulnerability than to actually exploit it in the real world. "No doubt it's a concern, but it's unlikely US aircraft will begin dropping out of the sky anytime soon," says John Bumgarner, research director for the US Cyber Consequences Unit, a cyber-security think tank. "It's just not very easy to launch some of these attacks, even if you know the vulnerabilities involved," he says in an interview. "Yes, they can happen. But it requires tons of reconnaissance and planning to pull it off." IOActive's trumpet blast, meanwhile, is hardly the first such warning. In November 2011, the US-China Economic and Security Review Commission revealed that unknown hackers had infiltrated command links to Landsat-7, a US Geological Survey Earth-imaging satellite launched in 1999, and Terra AM-1, which carried NASA climate change sensors. Neither satellite was damaged, although hackers on June 20, 2008, "achieved all steps required to command" NASA's Terra, "but did not issue commands," the commission said. Soon after, the President's National Security Telecommunications Advisory Committee reported in 2009 on cyber-threats to satellite networks, noting that "satellite and terrestrial networks share similar cyber-vulnerabilities." The IOActive report focused on the world's most widely used SATCOM terminals that connect with Inmarsat, a British satellite communications provider, and Iridium, a US-based provider. Even though newer satellites and SATCOM terminals have more secure communications available today than when Landsat or Terra were launched, the soaring demand for satellite bandwidth means US government and military communications are increasingly using commercial satellite data pathways that are somewhat less well protected, satellite communications experts say. Indeed, proprietary satellite communications have ceded ground in recent years to lower-cost, easier-to-use Internet Protocol or "IP-based" systems that have increased usability – but also the vulnerability of SATCOM systems overall, some experts say. "Reducing the technical expertise required to connect to a satellite has the unintended consequence of making it easier for hackers to connect to a satellite," writes Jason Fritz, an Australian cyber-expert at Bond University in Queensland, in an e-mail interview. SATCOM "vendor brochures often advertise security and encryption," he notes, "but in some cases it is up to the individual user to enable these features and follow proper procedures." Dr. Fritz's view was confirmed by a satellite industry official who, speaking anonymously to protect his business ties, agrees that there are indeed cyber-security "gaps among some of the more casual users" of SATCOM links. While high-security settings are usually available on such equipment, it is frequently not used or default passwords are not changed – lapses that increase vulnerability to attacks. "This equipment has been developed and designed to be so secure that if the features that are there in the systems are coherently implemented by the users, they are among the most secure systems in the world," says the industry official. "The big gap is among more casual users who are not in the middle of a fire-fight." But that gap is appearing at the very time that cyber-attackers are intensifying their hunt for vulnerabilities to exploit, SATCOM security experts say. "The line between SATCOM networks and IT networks have blurred substantially," said Christopher Fountain, president of Kratos SecureInfo, a Chantilly, Va., cyber-security company. He told Milsat Magazine, a satellite industry trade publication, in July that increased use of Internet-based satellite communications protocols is "bringing additional cyber-security risks. This is against an environment where cyber-attacks and threats continue to increase." According to the Kratos SecureInfo website, "cyber-attacks are increasing at an exponential rate and satellite communications are a prime target." In response, the satellite industry is ramping up its public face and focus on cyber-threats. In February, the Global VSAT Forum (GVF), which represents the satellite communications industry worldwide, announced a new "cyber-security task force" to address the threat. "We're working with industry to thwart indicators of cyber-attacks being made on the entire telecommunications sector," says David Hartshorn, GVF secretary general, in an interview. To read more click **HERE**

Hackers Claim to Have Found New OpenSSL Flaw Similar to Heartbleed

SoftPedia, 28 Apr 2014: A group of hackers claims to have identified a new vulnerability in the latest version of OpenSSL. They say they've found a security hole that's similar to the now infamous Heartbleed bug in OpenSSL 1.0.1g, but experts are questioning their claims. "We have just found an vulnerability in the patched version OpenSSL. A missing bounds check in the handling of the variable DOPENSSL_NO_HEARTBEATS. We could successfully Overflow the DOPENSSL_NO_HEARTBEATS and retrieve 64kb chunks of data again on the updated version," the hackers wrote on Pastebin. They haven't made the exploit, which is allegedly written in Python, public. The hackers are confident that they can leverage the vulnerability for their own gain for a long time before it gets patched. On the other hand, they're also willing to sell it for 2.5 Bitcoins ($1,069 / €780) or 100 Litecoins ($973 / €725). Not much is known about the group that's advertising the exploit. Their contact email address is BitWasp@safemail.net. "We are team of five people, and we have coded nonstop for 14 days to see if we could find a workaround, and we did it! We have no reason to make it public when the vendors will go for a update again," they noted. The only proof they've made available is a screenshot which shows what appears to be a response from a server. However, that doesn't prove much and security experts are skeptical about the hackers' claims. "They say: 'A missing bounds check in the handling of the variable DOPENSSL_NO_HEARTBEATS'. That's not a variable, the 'D' is not actually part of the name, and it's a compile-time macro that configures whether heartbeats will be compiled in or not," noted security expert and programmer Jann Horn on the Full Disclosure mailing list. "And because it's a compile-time thing, it's nothing that an attacker could ever influence," Hord added. Some believe that this is simply a money-making scam. The BitWasp@safemail.net was used in the past by a group that offered to sell user information and source code from Mt. Gox and CryptoAve. In addition to posting their claims on Pastebin, the hackers are also advertising the exploit on a couple of Chinese forums. Chinese experts also appear to be skeptical. Similar to Horn, some of them highlight the fact that the DOPENSSL_NO_HEARTBEATS variable doesn't exist. The Heartbleed bug, which is said to have impacted a large number of websites, has been patched by most companies. To make sure we don't see another similar vulnerability any time soon, some of the world's largest tech companies have announced their support for a Linux Foundation project called the Core Infrastructure Initiative. To read more click **HERE**

Adobe Flash Player 13.0.0.206 Now Available for Download
SoftPedia, 28 Apr 2014: Adobe has just rolled out a new version of Flash Player that comes to fix some of the issues spotted in the previous builds and thus improve the overall experience on all platforms. There are no release notes available right now, but it's safe to assume that Adobe Flash Player 13.0.0.206 is supposed to fix bugs and improve stability and reliability, so everyone should get the new version as soon as possible. There are no big feature changes in this update, so you might not see anything different at the first sight, but it's the under-the-hood work that's more important right now. Just like the previous versions, Adobe Flash Player 13.0.0.206 continues to work flawlessly with all modern browsers on the web right now, including Internet Explorer, Opera, and Chrome, while also offering support for mobile devices to access rich content wherever you are. As far as mobile devices are concerned, Flash player also comes with multitouch and accelerometer support, so it takes full advantage of features implemented in new devices. Overall, there's no doubt that this is a necessary update for everyone running Adobe Flash Player right now, so use the links below to download the new version and fix any bugs that might exist in your version. To read more click **HERE**

Unrevoked Security Certificates Put Users in Danger of Heartbleed
SoftPedia, 28 Apr 2014: The world's big companies are failing to revoke their old security certificates despite the importance of such a step following the Heartbleed bug. According to Netcraft, companies such as Yahoo, Facebook and LinkedIn have failed to revoke all of the certificates they reissued in response to the Heartbleed bug, which makes users susceptible to man-in-the-middle attacks. When Heartbleed was exposed, about 17 percent of all SSL web servers were vulnerable to the bug. The vulnerability had been built into OpenSSL for about two years and it's impossible to know if Heartbleed has been exploited or not since no traces are left behind on affected servers. The bug made it possible for hackers to steal a server's private keys, which allowed them to impersonate an affected website using its own SSL certificate. A good portion of the certificates that could have compromised were reissued, but a few of them have actually been revoked. In fact, these old certificates are best to be revoked to make sure that everything is safe. This is most effective when the revocation is included in the Google CRLSets. Basically, those who haven't taken these steps are still exposing their users to the vulnerability. Yahoo, for instance, offered the Heartbleed TLS extension before the disclosure of the bug, but has now changed its certificate. The previous certificate used on login.yahoo.com, however, has not been revoked. This means that if you use any of Yahoo's tools, you could still be vulnerable to man-

in-the-middle attacks until it is revoked. Although, considering Yahoo's many fail moments, no one's really surprised by the slip, other sites are also making the same error. Twitter, LinkedIn, Facebook, Apple, FedEx, PayPal and American Express are all on the same list of services that have failed to take all the necessary steps and that have limited themselves to patching up the servers and reissuing a new certificate, while leaving the old one to rot or be used by ill-willed hackers. The reasons that the old certificates have not yet been revoked can be many. On the one hand, some sites may believe this move to be useless, while others may not actually think this is necessary. There are also site admins that may want to wait a few weeks to make sure everything is ok with the new certificate, which involves delaying the revocation process for at least a little while. To read more click **HERE**