The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

14 May 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

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

May 12, IDG News Service – (International) **Microsoft extends deadline for Windows 8.1 Update requirement.** Microsoft announced that Windows 8.1 consumers have until June 10 to upgrade to Windows 8.1 Update before users stop receiving security updates on the former operating system, extending the previous deadline of May 13. Source: http://www.networkworld.com/news/2014/051214-microsoft-extends-deadline-for-windows-281502.html

Experts Advise Estonia to Stop Using Its E-Voting System Due to Security Concerns
SoftPedia. 14 May 2014: Security experts have analyzed the electronic voting system used by Estonia and have found a number of vulnerabilities that could be leveraged to influence elections. The warning has been issued just days before the European Parliament elections. In Estonia, as many as a quarter of all voters use the Internet to cast their ballots. This means that a cyberattack on the system could have serious consequences. Harri Hursti, a security researcher from Finland, and a team from the University of Michigan have identified several problems after analyzing the publicly available source code, documents and software. For instance, they've found that the security architecture used by Estonia for the e-voting system is out of date. Furthermore, those involved in maintaining the electronic voting system don't focus too much on security practices, not even basic ones. They're downloading software over unsecured connections, and they're typing passwords without being concerned that they're being filmed. The vulnerabilities present in the system could be exploited for server-side attacks in which malware can be used to rig the vote count, and client-side attacks in which a bot overwrites the voter's choice. "Despite positive gestures towards transparency — such as releasing portions of the software as open source and posting many hours of videos documenting the configuration and tabulation steps — Estonia's system fails to provide compelling proof that election outcomes are correct," experts warned. "Critical steps occur off camera, and potentially vulnerable portions of the software are not available for public inspection." Given enough resources, a foreign power such as Russia, could alter the outcome without being detected, researchers warn. This wouldn't be the first time Russia targets Estonia in cyberspace. In 2007, a massive denial-of-service (DOS) attack launched by Russia severely disrupted Estonia's critical infrastructure. "While we believe e-government has many promising uses, the Estonian I-voting system carries grave risks — elections could be stolen, disrupted, or cast into disrepute," experts noted in their report. "In light of these problems, our urgent recommendation is that to maintain the integrity of the Estonian electoral process, use of the Estonian I-voting system should be immediately discontinued." The researchers provided Estonian authorities with the results of their work on May 10, five days before the elections. However, Estonia's National Election Committee contests these findings, arguing that the system has been already used in six elections without any incident. Despite being warned, the country is confident in its system and refuses to suspend online balloting. To read more click **HERE**

Microsoft Launches Critical Internet Explorer Security Update

SoftPedia, 14 May 2014: May 2014 brought us eight different security bulletins supposed to fix 13 different vulnerabilities in Microsoft software, including two privately-reported flaws in Internet Explorer. All versions of Microsoft's in-house browser got patched today, so everyone running Windows and using Internet Explorer should hurry up to deploy the released fixes as soon as possible. According to Microsoft, the exploit would involve a compromised website which could be used to break into the computer using the aforementioned Internet Explorer vulnerability, so just try to avoid clicking on suspicious links until you deploy today's patches. "The most severe vulnerabilities could allow remote code execution if a user views a specially crafted Web page using Internet Explorer. An attacker who successfully exploited the most severe of these vulnerabilities could gain the same user rights as the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights," Microsoft says. There's no word on any potential attacks that might have been spotted until now, but there's no doubt that Windows users could be under attack if they do not fix the Internet Explorer flaw as soon as possible. According to the same advisory released today, the MS14-029 is currently being shipped to all computers running Internet Explorer, with Windows XP representing the only exception. Microsoft officially pulled the plug on Windows XP on April 8, so the company is no longer rolling out fixes and security updates for this particular OS version. As a result, those still running Windows XP and using Internet Explorer to browse the web should consider switching to a different browser such as Google Chrome and Mozilla Firefox as soon as possible, since no updates will be shipped to their computers. The patch is being flagged as critical for Internet Explorer on Windows clients, Microsoft said, and as important on Windows server. "This security update is rated Critical for Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10 and Internet Explorer 11 on Windows clients, Moderate for Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10 and Internet Explorer 11 on Windows servers," it said. As it's the case of all the other patches released by Microsoft on the second Tuesday of each month, this Internet Explorer fix is being shipped via Windows Update, so an Internet connection and Windows Update turned on should be all you need to stay secure. To read more click **HERE**

Microsoft Rolls Out Flash Player Update for Internet Explorer

SoftPedia, 14 May 2014: Internet Explorer is one of the software solutions that got fixed today as part of Microsoft's Patch Tuesday cycle, with Microsoft rolling out not only security updates addressing vulnerabilities, but also a new Flash Player improvement to fix recently-found glitches. Both Internet Explorer 10 and 11 received the new update this morning and it's essential for those who are using it on a regular basis to deploy the patch as soon as possible. "On May 13th, a security update for Adobe Flash Player in Internet Explorer 10 and 11 on supported editions of Windows 8, Windows 8.1 and Windows Server 2012 and Windows Server 2012 R2 is also available. This update addresses the vulnerabilities in Adobe Flash Player by updating the affected Adobe Flash binaries contained within Internet Explorer 10 and Internet Explorer 11," Microsoft explained. Of course, the patch is being delivered to users via Windows Update, so it's enough to connect the computer to the Internet and wait until the download and installation are performed automatically. Keep in mind that only Windows 8, 8.1, and 8.1 Update client operating systems are getting this update, so in case you're running any other OS version right now, Flash Player isn't patched by Microsoft via Windows Update, which means that you need to get the released fixes manually. To read more click **HERE**

Microsoft Releases Windows, Office May 2014 Security Updates

Softpedia, 14 May 2014: Microsoft today rolled out this month's Patch Tuesday updates to fix a total of 13 different vulnerabilities in its software, including Windows, Internet Explorer, and Office. According to an advisory released by the company this morning, the eight security bulletins, two of which are rated critical and six considered to be important, fix flaws in NET Framework, Office, SharePoint, Internet Explorer, and Windows which Microsoft says you need to patch as soon as possible. Microsoft Office is one of the software solutions that received updates this Patch Tuesday and as promised, Office 2003 is being left out from this month's rollout. The software giant says that the

proofing tools in Microsoft Office 2007, 2010, and some RT versions are "vulnerable to a bug in the way Office checks Chinese grammar, specifically in how it loads a particular DLL." "By putting a malicious DLL with a particular name in a particular network directory, an attacker could get users to load attack code," the company explained. A second vulnerability only affects Office 2013 and implies that the user visits a malicious websites which can be used to obtain access tokens from Office. An update aimed at Internet Explorer users is said to be "the most critical" released this Patch Tuesday and everyone is recommended to deploy it as soon as possible. "All supported versions of Internet Explorer on all supported versions of Windows (this no longer includes Windows XP) are vulnerable to two memory corruption vulnerabilities which could result in remote code execution. Microsoft says they are aware of limited attacks that attempt to exploit one of the vulnerabilities in Internet Explorer," Microsoft says. Last but not least, security bulletin MS14-027 is supposed to fix a problem in Windows that would expose user data in the case of an exploit taking advantage of a Windows Shell bug that causes improper handling of file association. All versions of Windows are vulnerable to attacks, so Microsoft is recommending everyone to patch as soon as possible. "All versions of Windows are vulnerable to an elevation of privilege vulnerability when the Windows Shell improperly handles file associations. A successful attacker could run code in the LocalSystem context. Microsoft says they are aware of limited attacks that attempt to exploit this vulnerability," it says. As usual, all patches are being delivered via Windows Update, so it's enough to connect your computer to the Internet and wait until they are automatically downloaded and installed. Some might require a system reboot. To read more click **HERE**

Adobe Fixes Flash Player and Reader Vulnerabilities Reported at Pwn2Own 2014

SoftPedia, 14 May 2014: Adobe has released security updates to address a total of eleven vulnerabilities affecting the Mac and Windows versions of Adobe Reader and Acrobat 11.0.06 (XI) and earlier. The company has also fixed six security holes affecting Adobe Flash 13.0.0.206 and earlier variants for Windows and Mac. The vulnerabilities are considered critical and they've been assigned a priority rating of 1, which means that they're either being targeted, or they have a high risk of being targeted. Adobe recommends system administrators to update installations as soon as possible, preferably within 72 hours. It's worth noting that the Flash Player vulnerability disclosed by VUPEN at Pwn2Own was addressed by Adobe with the security updates released on April 8, 2014. To read more click **HERE**

China Developing a Linux-Based Windows XP Alternative, Hopes Microsoft Users Will Jump Ship

SoftPedia, 13 May 2014: Windows XP is officially an unsupported operating system, so it no longer receives updates and security patches from Microsoft, but that doesn't necessarily mean that users are ready to give up on it. China is one of the countries where Windows XP continues to be one of the leading platforms, with some stats pointing towards a 70 percent market share owned by the OS version launched by Microsoft in 2001. The local government has apparently found a solution to move users off Windows XP by developing its own Linux-based alternative which would not only be offered with a freeware license, but also work on low-spec PCs, such as the ones that are currently powered by XP. A report by Global Times that's citing a statement of a Chinese official reveals claims that work on this new Linux-based OS has already been started, with local authorities hoping that Windows XP users would actually give it a chance and abandon their existing operating systems that are more or less open to attacks. Zhang Feng, chief engineer of China's Ministry of Industry and Information of Technology (MIIT), said in a statement that it's essential for the country's security to convince users to give a shot to these locally-developed platforms, but it remains to be seen how many people are actually prepared to give up on Windows. "We want users to pay attention to the potential security risk brought by their Windows XP system as Microsoft ceased providing further patch services. At the same time, the ministry will work on developing China's own computer system and applications based on Linux and we hope that the users will give more support to these domestically made products," he was quoted as saying by the source. One of the main issues is obviously app compatibility, as many of the apps that are currently available on Windows do not work on Linux. At least, not for the moment. Chinese officials admit that this could be a problem that could limit the adoption of the new locally-developed operating system, but explained that the 1 percent market share currently held by Linux is

very likely to experience a significant boost if the final product is truly effective. China is one of the countries that have asked Microsoft to extend Windows XP support until all local computers are upgraded to a new OS version and even referred to Windows 8 as a very expensive platform that isn't worth the money. Microsoft, however, refused to make any exception and pulled the plug on Windows XP all over the globe on April 8. To read more click **HERE**

Counterfeit Apple Chargers Can Kill You, Stop Buying Them, Says Tech Whiz

SoftPedia, 13 May 2014: People don't care half as much about chargers as they do about the quality and originality of the smartphone that gets juice from it, but electronics whiz Ken Shirriff assures us this is a terrible mistake. In a lengthy blog post, Shirriff, who works at Google according to his G+ profile, explains the major differences in build quality between a genuine Apple charger and fakes. Apple itself once warned people that they should only use original adapters, and even offered to rid the market of the counterfeit chargers to protect users, after a couple of incidents. "Apple sells their iPad charger for $19 [€13], while you can buy an iPad charger on eBay for about $3 [€2]. From the outside, the chargers look the same," Shirriff explains. "Is there a difference besides the price? In this article, I look inside real and counterfeit chargers and find that the genuine charger has much better construction, power quality, and most importantly safety. The counterfeit turns out to be a 5 watt charger in disguise, half the power of a genuine charger," he writes. The post in question is essentially a teardown report of two chargers, one genuine, one a blatant knockoff. Besides some differences in text and a fake certification claim that you'd need to know about before you could spot it, the two chargers look virtually identical. However, pry them open and you'll be in for a surprise (again, if you know your electronics). "Opening up the chargers reveals big differences between them. The genuine charger on the left is crammed full of components, fitting as much as possible into the case," Shirriff notes. He shows how the fake unit is much simpler in design, featuring far less and smaller components, with a great deal of empty space between them. In contrast, "The Apple charger uses larger, higher-quality components (in particular the capacitors and the transformer)," he points out. He proceeds to explain what every component does and how these have a huge effect on power quality and safety. One of the more obvious differences is the lack of insulation inside the knockoff adapter, which can pose risks. "The build quality of the Apple charger is much higher. In the counterfeit charger, some components are visibly crooked or askew. While this doesn't affect the circuit electrically, it indicates a lack of care in construction," adds Shirriff. He concludes, saying, "Safety probably isn't something you think about when you plug in your charger, but it's important. Inside the charger is 170 volts or more with very little separating it from your iPad and you. If something goes wrong, the charger can burn up (below), injure you, or even kill you." To read more click **HERE**