Information Security Awareness

Program by

Information Security Education & Awareness
Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India.

www.infosecawareness.in

Feb-Mar 2013

InfoSec Tip

Do not download Software from untrusted sources

Computer users often download software from Internet and install them. These software may contain virus, worms, Trojan Horses etc. Installing unnecessary applications and software may compromise the security of the system. Even if the software or applications are found to be legitimate, it is suggested that these may be installed only if it is essential.

Let us see how this turns to benefit attackers.

Hackers have found a flaw in Java software, which allows them to enter into the system and install any malicious applications on the target system. Users who are using latest java release 7u1-5 are told to disable java plugins from their browsers. Assume that a user has not followed the advisory from original software developers, then the situation is something like this, Whenever you visit a website controlled by an attacker, it automatically detects your java version and exploits the same. Once the exploit is successful the attacker installs malicious software and gain access to your PC. Once the attacker installs the malware he/she can do the following. Attacker can capture your conversations if you have microphone, can capture video from your webcam, take screenshots from your system, download and upload files to your PC, etc.

Tips

- Scan the software before installing with up-to-date Antivirus
- Do not install unnecessary software, which are not required
- Always update the applications and software installed on the PC
- Always follow the standard advisory from original developers of software

InfoSec Quote

I don't hate technology, I don't hate hackers, because that's just what comes with it, without those hackers we wouldn't solve the problems we need to solve, especially security.

- Fred Durst

InfoSec Cartoon

Never keep any of your sensitive documents on your tabletop.

For Virus Alerts, Incidents and Vulnerability Reporting
certin
Handling Computer Security Incidents

Executed By :
Centre for Development of Advanced Computing
Hyderabad

InfoSec Quiz

1. ---------- is an entity that issues Digital Certificates in a Public Key Infrastructure.
   (a)National Informatics Centre (b)VeriSign (c)komodo (d)Certifying Authority

2. Wardriving is an act of searching ----------
   (a)Mails (b)Wired networks (c)Wireless Networks (d)none of the above

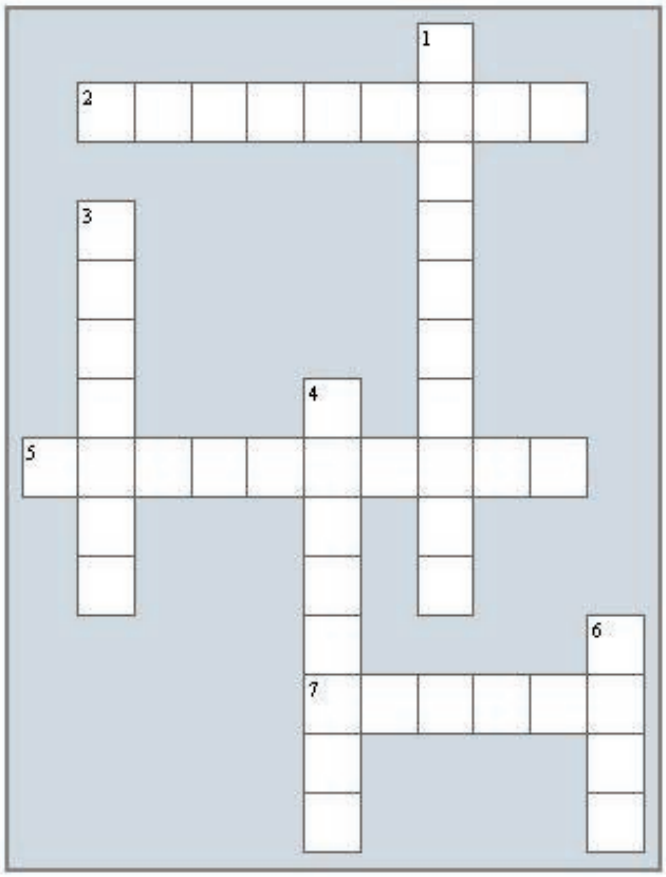
3. IT act 2000 has -------- chapters
   (a)10 (b)11 (c)12 (d)13

4. ---------- is a worm
   (a)hikit (b)Win32.worm.stuxnet.A (c)duqu (d)All of the above

5. ---------- is not a free and open source operating system
   (a)fedora (b)ubuntu (c)Windows 7 (d)Kubuntu

logon to www.infosecawareness.in to participate in InfoSec Contest

InfoSec Crossword



Across :

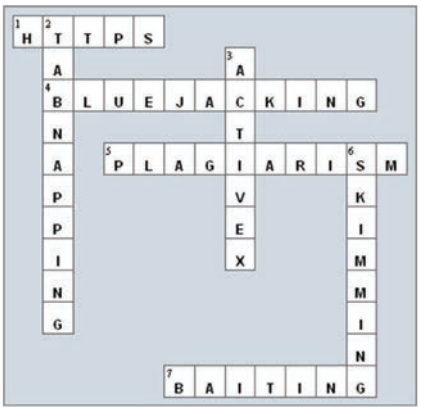
2. What's another name for crackers -- malicious hackers who infiltrate secure systems in order to steal information or cause damage?
5. ____ is the use of computers and computer networks as a means of protest to promote political ends
7. ____ is a popular webserver used on internet

Down:

1. Going behind somebody through the access doors without using own access card
3. Computer worms, viruses and trojans are grouped in to one category called
4. ____ is used to block unwanted traffic from Internet
5. ____ is a famous Trojan Horse that steals banking information.

Last edition Contest Answers

Crossword Answers



Quiz Answers

1. **d**
2. **a**
3. **a**
4. **d**
5. **b**

Last edition Contest Winners

InfoSec Crossword Winner

Ravi.K

InfoSec Tools

WehnTrust

Though Windows XP is more than a decade old Operating System it has still ~30% share in enterprise PCs. Ofcourse, if in these ten years hackers have reached new heights, security researchers also have chasen them to full. Most noticeable security feature is Address Space Layout Randomization (ASLR). This kind of exploit protection is not available on Windows XP.

Overview :

WehnTrust is a Host-based Intrusion Prevention System (HIPS) for Windows 2000, XP, and Server 2003. It includes support for exploit mitigations that are designed to make exploitation more difficult by preventing the use of specific exploitation techniques and by making exploitation unreliable.

How it works

WehnTrust randomizes the base addresses of memory allocations to make it more difficult to exploit software vulnerabilities such as buffer overflows. This technique is commonly known as Address Space Layout Randomization (ASLR) and was originally conceived by the PaX team. Microsoft has recently incorporated support for ASLR into Windows Vista and Windows Server 2008. In addition to ASLR, WehnTrust generically mitigates SEH overwrites by dynamically validating a thread's exception handler chain prior to allowing exceptions to be dispatched.

Using WehnTrust in combination with hardware-enforced DEP (non-executable pages) as included with Windows XP SP2 and Windows Server 2003 provides the greatest level of security. Non-executable pages help to counter some of the inherent weaknesses of ASLR.

WehnTrust provides protection to Windows XP and Server 2003 PCs from being exploited. The tool has following three main features:

1. IT provides ASLR which makes exploitation very difficult.
2. SEH Overwrite Prevention
3. Format String Vulnerability Prevention

User need not do any configuration after installing this software. If any attempt to exploit is prevented by WehnTrust then it logs it which can be viewed in Event Viewer.

The tool can be downloaded free of cost from ***http://wehntrust.codeplex.com/***

The commercial version of the tool is available only at ***http://www.wehnus.com/products.pl***

PhotoRec

PhotoRec is file data recovery software designed to recover lost files including video, documents and archives from hard disks, CD-ROMs, and lost pictures (thus the Photo Recovery name) from digital camera memory. PhotoRec ignores the file system and goes after the underlying data, so it will still work even if your media's file system has been severely damaged or reformatted.

PhotoRec is free - this open source multi-platform application is distributed under GNU General Public License (GPLV v2+). PhotoRec is a companion program to TestDisk, an application for recovering lost partitions on a wide variety of file systems and making non-bootable disks bootable again.

For more safety, PhotoRec uses read-only access to handle the drive or memory card you are about to recover lost data from. As soon as a pic or file is accidentally deleted, or you discover any missing, do NOT save any more pics or files to that memory device or hard disk drive; otherwise you may overwrite your lost data. This means that while using PhotoRec, you must not choose to write the recovered files to the same partition they were stored on.

Operating Systems Supported:

PhotoRec runs under

- DOS/Win9x
- Windows NT 4/2000/XP/2003/Vista/2008/7
- Linux
- FreeBSD, NetBSD, OpenBSD
- Sun Solaris
- Mac OS X

and can be compiled on almost every Unix system.It can recover lost files at least from

- FAT
- NTFS
- exFAT
- ext2/ext3/ext4 filesystem
- HFS+

Reference: *http://www.cgsecurity.org/wiki/PhotoRec*
Download: *http://www.cgsecurity.org/wiki/TestDisk_Download*

Guess the tip which suits the cartoon picture and win prizes

Log on to www.infosecawareness.in to send the tip

InfoSec Concept

USB Storage Device Security

USB flash drive is a data storage device used for storage, back-up and transfer of computer files. USB mass storage devices like pendrives, micro SD cards, external storage devices are used to store images, audio, video etc. These devices are relatively small, durable and reliable compared to floppy disks and CD-ROMs. They have replaced Floppy disks which were used earlier. USB devices are superior in terms of speed and storage capacity.

The popularity of USB storage devices has attracted attackers to use these as a medium to spread viruses, worms and trojans. USB devices are used by attackers to perform malicious activity on the targets computer.

One of the options for an attacker is to use USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware. Once malware is installed in the victims computer, the installed malware can detect whenever a new USB drive is plugged into the computer and the malware on the infected PC infects that USB drive, which when inserted into another PC the malware tries to get installed on that PC as well. In this way the malware spreads from one system to other.

Attackers may also use their USB drives to steal information from a computer which is not even connected to internet. The most obvious security risk for USB drives is that they are easily lost or stolen. If the data was not backed up, the loss of a USB drive can mean hours of lost work. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

News about USB attacks:

Stuxnet a highly sophisticated computer worm discovered in june,2010 attacked Iranian uranium enrichment infrastructure. The worm initially spread using infected removable drives such as USB flash drives. Stuxnet attacked windows systems using an unprecedented four zero-day attacks. The malware has created a huge loss to Iranian government.

Flame, also known as Flamer is a computer malware discovered in 2012 that attacks computers running Microsoft Windows operating system. Flame can spread to other systems via USB stick. It can record audio, screenshots, Keyboard activity and network traffic. This data along with locally stored documents is sent on to one of several command and control servers that are owned by attackers.

The following are the guidelines to safe use of USB storage devices.

There are steps you can take to protect the data on your USB drive and on any computer that you might plug the drive into.

1. Take advantage of security features

Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost.

2. Use and Maintain security software and keep all software up to date

Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions up-to-date.

3. Use different drives for personal and business use

Do not use personal USB drives on computers owned by your organiza tion, and do not plug USB drives containing corporate information into your personal computer

4.Do not plug an unknown USB drive into your computer

If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into your computer to view the contents or to try to identify the owner. There is a chance that your system may get infected by just opening the USB drive you found.

5. Disable Autoplay

The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically.

Do's and Dont's

- Don't leave your flash drive in extreme temperatures.
- Below freezing temperatures or excessive heat can damage your flash drive, leaving it unusable. Always keep it in a safe place, preferably at room temperature.
- Do save your work to your flash drive frequently.
- If you're writing an important paper which is directly stored in the USB drive, get in the habit of saving your work every 10 minutes. The sudden loss of power or accidentally closing out the program you're using can be extremely frustrating, but even more so if you haven't saved your progress and then have to go back and write it all over again.
- Don't use a USB stick that you found or receive for free.
- Always buy from trusted sources and never collect any pendrives which were found. Always clean the USB drive with latest Antivirus software when you bought for the first time.
- Don't allow someone else to put a USB stick of unknown origin into your computer.
- Sometimes the USB stick from not trusted sources may contain malware which can harm your computer. If necessary scan the USB drive with latest Antivirus software and use them.

References:

http://en.wikipedia.org/wiki/Universal_Serial_Bus
http://www.infosecawareness.in
http://labs.bitdefender.com/2012/05/cyber-espionage-reaches-new-levels-with-flamer

InfoSec Latest News

Spam hits Indian users of Skype

A "malicious spam" has hit the internet-based audio-video communicator 'Skype' in the Indian cyber-space and anti-hacking sleuths have asked users to remain alert and cautious. "A malicious spam campaign is on the rise targeting Skype users by sending instant message which appears to come from friends in the Skype contact list," a government advisory to 'Skype' users in the country said.Cyber security experts found the malware content has been lurking in the vicinity of cyber networks of Indian users who use this popular Voice-over Internet Protocol (VoIP) service.

A number of Indians use 'Skype' to communicate with their friends, relatives and other contacts within and outside the country. The government agency mandated to counter such threats-- the Computer Emergency Response Team (CERT-In) under the Communications and Information Technology ministry, said the spam "eventually controls the victim machine by opening a backdoor and communicating to a remote http server.

"The worm reported as stealing user credentials, engaging in click fraud activities and pose as ransom ware," the agency said. Cyber sleuths have also recommended a number of counter- measures in this regard as it asked the users of this form of web telephony not to "follow unsolicited web links or attachments in Skype messages and install latest security updates to Skype". "Download the latest version of the Skype from the trusted markets, install and maintain updated anti-virus software at gateway and desktop level, use caution when opening attachments and accepting file transfers, disable auto play feature as a safe practice. "Use caution when clicking on links to web pages and protect yourself against social engineering attacks," the agency advised internet users in the country.

References :

http://articles.economictimes.indiatimes.com/2012-10-30/news/34817419_1_skype-users-malicious-spam-indian-users

European banks lose $47m in cyberattacks

More than 36 million euros ($47 million) were stolen earlier this year from some 30,000 bank accounts in Europe in a cyberattack dubbed "Eurograbber", according to a report published by two companies that focus on internet security. In Spain alone, the cyberthieves stole 5.8 million euros ($7.5 million) from 11,352 accountholders at seven banks, according to the report from Check Point Software Technologies Ltd. and Versafe. The attack affected computers and cell phones between January and August of this year, Mario Garcia, general director of Check Point Espana, confirmed to EFE.

It was Check Point that in August reported the attack to the European police and alerted the affected banks. Garcia explained the procedure the virus used to invade the banking system: after accessing certain links, the malware installs itself in a computer and remains inactive until the user connects online to their bank account. It is then that the communication of the user with the bank is intercepted and replaced.

The malware, which simulates being a bank, sends a warning to the user about updating and improving online security and asks for their cell phone number, by which it also infects that device and interferes with the messages that banks send as part of the authentication process. With the information and the transaction processing number, the cyberattackers can execute cash transfers parallel to those of the actual customer. "If you transfer, for example, 100 euros, they can steal another such amount and you don't see any change, either on the computer screen or on the cell phone," Garcia said.

The amounts stolen ranged from between 500 to 250,000 euros ($650 to $327,000) and were removed from individual and corporate accounts in Italy, Spain, Germany and The Netherlands.

InfoSec Security Alerts

Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible.
CVE-2012-4681

Description

This Security Alert addresses security issues CVE-2012-4681 (US-CERT Alert TA12-240A and Vulnerability Note VU#636312) and two other vulnerabilities affecting Java running in web browsers on desktops. These vulnerabilities are not applicable to Java running on servers or standalone Java desktop applications. They also do not affect Oracle server-based software.
These vulnerabilities may be remotely exploitable without authentication, i.e., they may be exploited over a network without the need for a username and password. To be successfully exploited, an unsuspecting user running an affected release in a browser will need to visit a malicious web page that leverages this vulnerability. Successful exploits can impact the availability, integrity, and confidentiality of the user's system.
In addition, this Security Alert includes a security-in-depth fix in the AWT subcomponent of the Java Runtime Environment.
Due to the severity of these vulnerabilities, the public disclosure of technical details and the reported exploitation of CVE-2012-4681 "in the wild," Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible.

Supported Products Affected

Security vulnerabilities addressed by this Security Alert affect the products listed in the categories below. Please click on the link in the Patch Availability column or in the Patch Availability Table to access the documentation for those patches.

Affected product releases and versions:

Java SE	Patch Availability
JDK and JRE 7 Update 6 and before	Java SE
JDK and JRE 6 Update 34 and before	Java SE

Java SE fixes in this Security Alert are cumulative; this latest update includes all fixes from previous Critical Patch Updates and Security Alerts.

Source:*http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715 html*

WPS PIN BRUTE FORCE (WIRELESS ROUTERS AND MODEM)

Systems Affected

Most Wi-Fi access points that support Wi-Fi Protected Setup (WPS) are affected.

Overview

Wi-Fi Protected Setup (WPS) provides simplified mechanisms to configure secure wireless networks. The external registrar PIN exchange mechanism is susceptible to brute-force attacks that could allow an attacker to gain access to an encrypted Wi-Fi network.

Description

WPS uses a PIN as a shared secret to authenticate an access point and a client and provide connection information such as WEP and WPA passwords and keys. In the external registrar exchange method, a client needs to provide the correct PIN to the access point.

An attacking client can try to guess the correct PIN. A design vulnerability reduces the effective PIN space sufficiently to allow practical brute force attacks. Freely available attack tools can recover a WPS PIN in 4-10 hours.

For further details, please see Vulnerability Note VU#723755 and documentation by Stefan Viehböck and Tactical Network Solutions.

Impact

An attacker within radio range can brute-force the WPS PIN for a vulnerable access point. The attacker can then obtain WEP or WPA passwords and likely gain access to the Wi-Fi network. Once on the network, the attacker can monitor traffic and mount further attacks.

Solution

Update Firmware

Check your access point vendor's support website for updated firmware that addresses this vulnerability. Further information may be available in the Vendor Information section of VU#723755 and in a Google spreadsheet called WPS Vulnerability Testing.

Disable WPS

Depending on the access point, it may be possible to disable WPS. Note that some access points may not actually disable WPS when the web management interface indicates that WPS is disabled.

References

- Vulnerability Note VU#723755 - *http://www.kb.cert.org/vuls/id/723755*
- Wi-Fi Protected Setup PIN brute force vulnerability - *http://sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability/*
- Cracking WiFi Protected Setup with Reaver - *http://www.tacnetsol.com/news/2011/12/28/cracking-wifi-protected-setup-with-reaver.html*
- WPS Vulnerability Testing - *https://docs.google.com/spreadsheet/lv?key=0Ags-JmeLMFP2dFp2dkhJZGIxTTFkdFpEUDNSSHZEN3c*

Source: *http://www.us-cert.gov/cas/techalerts/TA12-006A.html*

InfoSec Workshops

@ Rourkela

@ Hyderabad

@ Mohali

@ Nahan

InfoSec Workshops

@ Tiruvananthapuram

@ Jalandhar

@ Shimla

@ Srinagar

Users views on the contest - Guess Tip Contest

Keeping internet security,and password security and PC security,and safe from cheating with password

----- Snehavasudevan

Secured network

-----Mustaphanasir

Protect Computer Network usage from others by Locking it with a password.

-----Anudeepreddy.A

Always use strong credentials to secure your Internet from unauthorized personnel

-----Rakhi.Wadhwani

User feedback on web portal

Content provided	Look & Feel	Navigation	Usefulness	Flow of the content
Excellent	Excellent	Excellent	Excellent	Excellent

Very nice ---- By Tushar

Good	Good	Good	Good	Good

Good website nice layout----By Chhavi

Excellent	Excellent	Excellent	Excellent	Excellent

Nice work keep it up ---- By Ashwini Shirke

Interested to organize InfoSec Workshop at your place? Please visit... http://infosecawareness.in/isea-pi or mail us at isea@cdac.in

Our Sincere thanks to Action Group Members for Guiding us

Dr.Kamlesh Bajaj, Data Security Council of India
Dr.B.K.Murthy, Director, Head of Division - HRD & NKN, DIT
Dr.Dhiren R Patel, Professor of Computer Science Department, IIT, Gandhinagar
Shri.Sitaram Chamarthy, Principal Consultant, TCS
Dr.N.Sarat Chandra Babu, Executive Director, C-DAC Bangalore

Comments & Feedback
*mail us at **isea@cdac.in***

For virus Alerts,Incident and Vulnerability Reporting
certin
Handling Computer Security Incidents

Editorial committee:
V.Muralidharan
Director
C-DAC Hyderabad
Mr.Ch.A S Murthy &
Mrs.Indraveni K,
C-DAC Hyderabad
Shri.S.K.Vyas,
Joint Director, DIT,
Shri G.V.Raghunathan,
Consultant,C-DAC Hyderabad

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded peogeamming in the application domains of Network Security, e-learning, Ubiqutous Computing, India Development Gateway (www.indg.in), Supply Chain Management and Wireless Sensor Networks.

Supported by
Department of Electronics & Information Technology
Government of India

सी डैक प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
JNTU Campus, Kukatpally, Hyderabad - 500 085. Tel: 040-2315 0115. Fax: 040-2315 0117.