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

InfoSec Newsletter

May-June 2015

Instant Messaging

InfoSec 9 Tools
Telegram

InfoSec 4 Concept

Participate in InfoSec
Quiz
Crossword
Guess the Tip

Supported by
For Virus Alerts, Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

सी डैक
CDAC
www.cdac.in

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
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)
E-mail : isea@cdac.in

InfoSec

Newsletter

May - June 2015

Credits

For Virus Alerts, Incident & Vulnerability Reporting
cert-in
Handling Computer Security Incidents

InfoSec Quiz

1. Which version of IM was invented first ?
   (a)Yahoo messenger (b)Jabber (c)ICQ (d)MSN Messenger (e)PLATO

2. What are the functions of IM management software ?
   (a)conversations logged and documented
   (b)Content filtering (c)None of the answers are correct (d)All are correc
   (e)Restricts

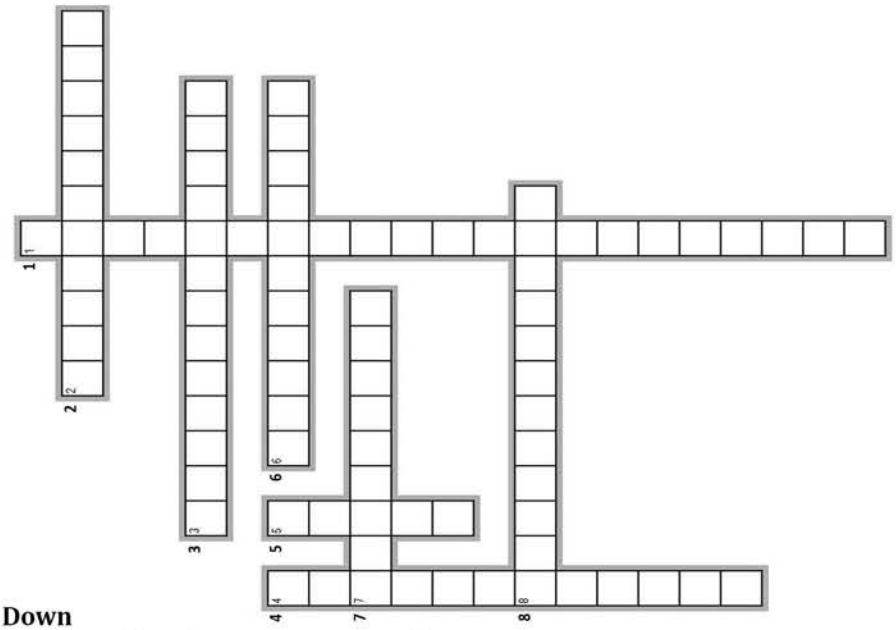
3. Instant messaging is
   (a)Also known as SMS (b)Also known as texting (c)Limited to 140 characters
   (d)known as short messaging
   (e)An online service where compatible software is used to communicate instantaneously

4. Which of the following is not an advantage of IM ?
   (a)Free software (b)Virus protection (c)Convenience (d)Real time
   (e)All the above

5. What is the main method used to execute an Instant messenger attack ?
   (a)An IM worm (b)An IM virus (c)Social Engineering (d)Trojan horse
   (e)Man-in-middle attack

logon to
www.infosecawareness.in/contest
to participate in Infosec Contest and **WIN PRIZES**

InfoSec Crossword



Down

1 Know the rules governing your chat experience
4 Do not let children use instant messaging chat rooms
5 Somebody persuading you to download and run a virus-infected piece of software

Across

2 There is no guarantee of privacy as conversations can be saved for use of-fline.
3 secretly listening to the private conversation of others without their con-sent
6 Always Verify that you receive on IM elsewhere. In particular, check any sec rity advice you get.
7 People online are not necessarily who they say they are or seem to be.
8 Some people are rude, disruptive, defamatory and obscene in online chat.

InfoSec Guess Tip

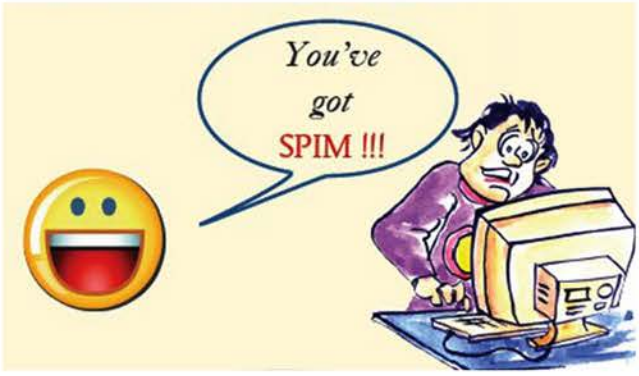
Guess the Tip which best suits the cartoon by logging in to
http://www.infosecawareness.in

InfoSec Tip

Avoid opening attachments and links in IM

Risks through Instant Messengers

SPIM



Spim is a short form of spam over Instant Messaging(IM), it uses IM platforms to send spam messages over IM. Like e-mail spam messages, a spim message also contains advertisements. It generally contains web links, by clicking on those links malicious code enters into your PC. Generally, it happens in real time and we need to stop the work and deal with spim as the IM window pop-ups, in the e-mail we have time to delete and we can delete all spam at a time, or we can scan before opening any attachments. This cannot be done in IM. So avoid opening attachments and links in IM.

More risks through Instant Messengers :

- The most evident is that your friends can see when you are online and jump into chat, it can be frustrating if you are busy in studies or learning something over Internet.
- The voice can be trapped while talking to your friends.
- Avoid opening attachments and links in IM
- You may receive unwanted texts or spam text messages which could contain inappropriate material.
- Text messages containing private, personal information could be sent to the wrong address.
- Video chats can be used to photograph or videotape without your knowledge.
- Photos and videos can reveal a user's appearance and place.
- Criminals are able to hide their identity in Instant messages through a false name, age and some grown up can pretend to be child.
- Some times strangers may offer free gifts through instant message with false information.

For more details visit
www.infosecawareness.in

INSTANT MESSAGING

Instant messaging has existed in some form or another for decades in Internet History. It is a process by which users on a computer network can quickly communicate with one another using short text-based sentences rather than using email. Each user has a piece of software that communicates with a common server that connects the chat sessions. Over the past few years, two distinct settings for the use of instant messaging have evolved.

The first is the corporate or institutional environment composed of many potential users but who are all under the same organizational umbrella. The second setting is individual users 'after work' or at home who do not have a mission-oriented commonality between them, but are more likely family and friends.

In the corporate setting, security risks are apparent from the outset. What stops a disgruntled employee from messaging some sensitive company data to a colleague outside the enterprise?

The reverse of that would be the example disgruntled employee downloading some virus or spyware onto his machine inside the corporate firewall to release as desired. Accordingly, organizational offerings have become very sophisticated in their security and logging measures.

Typically, an employee or organization member must be granted a login and suitable permissions to use the messaging system. This creating of a specific account for each user allows the organization to identify, track and record all use of their messenger system on their servers.

The specialized requirements of the organizational messaging system, however, run almost completely contrary to what an individual user may need. Typically non-organizational use instant messengers advertise their availability to the Internet at large so that others may know if that person is online. The trend has been too that manufacturers of instant messaging clients offer interoperability with other manufacturer's clients.

Limit interactions to users in a chat room

Features of Instant Messengers

- **Presence and Status Broadcasting -** Messengers attempt to maintain a social environment and always stay 'connected'.
- **Interoperability –** Many other manufacturers can interoperate with the example messenger.
- **Contact Lists -** Maintains lists of all desired contacts.
- **Client-Server Design –** Requires use of third party servers to provide chat functionality to messenger clients.
- **Logs Messages –** Messages and other events are recorded

Popular Instant Messaging Solutions in Mobiles/Tablets

Along with the boom in smart phones around the world, instant messaging applications created have been downloaded in almost every mobile device. The main reason why these apps are such a big hit with users is because they are easy to use and, more importantly, free.

Viber:

Developed by Viber Media, it is a proprietary cross-platform instant messaging voice over Internet protocol application for smart phones. In addition to text messaging, users can exchange images, videos and audio messages

LINE:

LINE is a Japanese proprietary application for instant messaging on smart phones and personal computers that allows users to make free voice calls and send free messages. Stickers and emoticons used in the app are popular among teenagers

KakaoTalk:

KakaoTalk is a multi-platform texting app created by South Korean team that allows iPhone, Android and BlackBerry users to send and receive messages for free. It has achieved 100 million subscribers since its release on March 18, 2010

WeChat:

WeChat, the mobile messaging application released by China's Internet giant Tencent, has 450 million monthly active users

WhatsApp:

WhatsApp Messenger is a cross-platform mobile messaging app that allows users to exchange messages without having to pay for them.

Kik:

Kik Messenger is an instant messaging application for mobile devices. Kik Messenger was released on October 19, 2010, by Kik Interactive, started by a group of students from the University of Waterloo, Ontario, Canada

Hike:

Hike is a communication app that offers both instant messaging and SMS under one roof, according to NDTV.com, an Indian TV network. It has been developed by Bharti Softbank, which is jointly held by India's Bharti Telecom and Japan's Softbank telecom provider. The app is the brainchild of Kavin Bharti Mittal

Risks in Mobile Instant Messaging

Virus and Worms
In 2014, 38% of Viruses in top 50 viruses and worms are targeted towards peer-to-peer or IM applications in Internet Communications. Most viruses are sent through file transfers, Public Instant Messaging (IM) clients also have publicized vulnerabilities, where flaws such as buffer overflows and boundary condition errors have been exploited to spread viruses, worms or denial-of-service attacks.

Spim
IMlogic says that 5% to 7% of IM traffic today is spim (instant messaging spam). Spim can be more disruptive than e-mail spam, as it is more intrusive (the pop-up spim interrupts the user) and generally of a more sexually offensive nature (leading to human resources and legal risk

Identity theft/authentication spoofing
Public IM systems let individuals create anonymous identities, which do not map to any identity and also IDs can be created even if the IDs and domains are not owned by that individual ("icici" or "john chambers," for example). Spoofing creates risk, as these IDs can be used maliciously, outside the control of the IT security department.

Firewall tunnelling
IM clients find ways to tunnel through firewalls, creating risk. Most IM services come through well-publicized ports (5190 for AOL Instant Messenger, 1863 for MSN and 5050 for Yahoo), but IM clients also can exploit any open port on the firewall, including those used by other applications (such as Port 80 for Web and HTTP traffic). Some clients also can connect via peer-to-peer connections or establish connections on randomly negotiated ports.

Data security leaks
Unmonitored content leaving the corporation without the knowledge of the information security department introduces legal and competitive risk (such as a CFO sending a confidential spreadsheet via IM without an audit trail). File transfer over IM is a powerful way to send information beyond the tracing capabilities of the IT department. The lack of content filtering and archiving makes it difficult for IT to discover potential breaches of policy or to hold individuals accountable.

Spim
IMlogic says that 5% to 7% of IM traffic today is spim (instant messaging spam). Spim can be more disruptive than e-mail spam, as it is more intrusive (the pop-up spim interrupts the user) and generally of a more sexually offensive nature (leading to human resources and legal risk

What we need to do?

Instant messaging applications add a lot of convenience, but few people take the time to think about security concerns. Every day, hackers are trying to gain access to our conversations. The good news is, there are certain things that can be done to make instant messaging safer.

Respect others and never misbehave over Internet Communication

Be Polite and kind during your chat sessions

Never download files through CHAT sessions from unknown persons

Avoid Exposing Private Information:

Developers have warned that many of the instant messaging applications make it easy for private information to be exposed and used for fraudulent purposes. Researchers at the University of California studied more than 120,000 free applications that are available for use on Android devices.

Many of the applications have parts of the code that are public, which means they could be modified easily for fraudulent purposes. The use of malicious code allows hackers and other individuals having malicious intent to send messages on behalf of someone, to get access to personal information and to replace the actual application with code designed for alternative purposes.

Despite the emphasis on Android apps, researchers believe that similar security concerns are valid for iPhone instant messaging options.

Encryption:

Several other instant messaging apps for smart phones were examined concerning the manner in which personal information is transferred and stored. WhatsApp, a market leader in the instant messaging niche, has been accused of transmitting address books and personal information unencrypted to the app server. Many bits of private information, including ID, are readily available for third parties to see and to utilize.

An even more troublesome trend has emerged recently. Certain applications were developed for the purpose of getting access to the instant messaging conversations of other people and for access to personal information. WhatsApp Sniffer is one such development. Such applications reveal once again how many security gaps instant messaging applications leave.

Facebook Chat? Think Again:

Various surveys were carried out and the conclusion is that Facebook Chat applications for mobile devices are one of the least safe options on the market. Encryption is not used to protect log in, which means that the password of an individual can easily be seen. The instant messaging conversations themselves are protected minimally. Yahoo! Messenger and the now defunct Windows Live Messenger are two other applications that fail protecting member conversations adequately.

Using Instant Messaging Apps Safely: What does it take?

The first and most obvious thing you can do to increase instant messaging safety and privacy is the selection of the right application. No two instant messaging apps are alike. Some developers put more emphasis on the protection of sensitive data. Data encryption is the first and the most basic way of data protection. Make sure that the apps you choose transfer all information in an encrypted form to the server. Some Internet apps such as Skype, Google Talk, AOL, Instant Messenger, similar major developments brag higher than usual security. Make sure you do your research before downloading your app of choice to keep your information secure.

Secure Instant Messaging

Secure instant messaging is a form of instant messaging wherein at the very least the users are exchanging chat messages the contents of which they have caused to be encrypted with keys they generate and control.

Recent news events have revealed that the NSA is not only collecting emails and im messages but also tracking relationships between senders and receivers of those chats and emails in a process known as 'meta data' collection.

'Meta data' refers to the data concerned about the chat or email as opposed to contents of messages. It may be used to collect valuable information. The wireless network that you use to do instant messaging is just as important.

Open networks like the ones available in cafés, at airports and bus stations are very easy to break through. When doing instant messaging, rely on a closed, password-protected Internet network. Instant messaging can be used to communicate with friends, business partners and acquaintances. Still, it is important to keep security concerns in mind. Though convenient, instant messaging can compromise personal information if the wrong app is chosen. Choose applications carefully and be smart in terms of what you share.

Almost by definition alone a secure messenger cannot be a social messenger. Therefore to be considered secure a messenger must behave differently than one used for more social purposes. Traits of a secure instant messenger include the ability to:

- Provide a 'stealth' online presence
- Send messages in cipher text not clear text form.
- Not log or store any information regarding any message or its contents.
- Not log or store any information regarding any session or event.
- Operate as a decentralized computing model not relying on third party servers for message security and handling.

Secure instant messengers aren't needed for every chat session but when there is a requirement for private, secure and untraceable messaging there is no other means to effect those requirements.

Popular Secure Instant Messaging Solutions in Mobiles/Tablets

Telegram:
Telegram is a cloud-based mobile and desktop messaging app with a focus on security and speed

Adium:
Adium is a free instant messaging application for Mac OS X that can connect to AIM, MSN, XMPP (Jabber), Yahoo, and more.

Bitbee:
BitlBee is a cross-platform IRC instant messaging gateway, licensed under the terms of the GNU General Public License

Jitsi:
JITSI (formerly SIP Communicator) is a free and open source multiplatform voice (VoIP), videoconferencing and instant messaging application for Windows.

InfoSec Tools

Telegram

a new era of messaging

Telegram is a messaging app with a focus on speed and security. It's super-fast, simple, secure and free.

Telegram seamlessly syncs across all of your devices and can be used on desktops, tablets and phones alike. You can send an unlimited amount of messages, photos, videos and files of any type (.doc, .zip, .pdf, etc.).

Telegram groups have up to 200 people and you can send broadcasts to up to 100 contacts at a time. Be sure to check our website for a list of Telegram apps for all platforms.

Telegram Applications

Mobile apps

- Telegram for Android
- Telegram for iPhone and iPad
- Telegram for WP
- Telegram for Firefox OS

Desktop apps

- Telegram for Windows/Mac/Linux
- Telegram for Mac OS X

Web apps

- Telegram Web-version
- Telegram Chrome app

Unofficial apps

- Telegram CLI for Linux
- Migram (alpha) for Windows Phone

Using Telegram API

Our API is 100% open for all developers who wish to create Telegram applications on our platform. Feel free to study the open source code of existing Telegram applications for examples of how things work here. Don't forget to register your application in our system.

Creating your Telegram Application

We welcome all developers to use our API and create applications on our platform.

There are only five things we require from all developers for the moment.

- Kindly obtain your own api_id for your application.
- Please don't use the name Telegram for your app or make sure you have the word unofficial in the title.
- Please do not use the official Telegram logo (white paper plane on a blue background) in your app.Please study our security guidelines and take good care of your users' data and privacy.
- Please make sure your users understand that your app is using our API and is part of the Telegram ecosystem, this must be mentioned in the app's description.

Obtaining api_id

In order to obtain an API id and develop your own application using the Telegram API you need to do the following:

- Sign up for Telegram using any application.
- Log in to your Telegram core: https://my.telegram.org.
- Go to 'API development tools' and fill out the form.
- You will get basic addresses as well as the api_id and api_hash parameters required for user authorization.
- For the moment each number can only have one api_id connected to it.

We will be sending important developer notifications to the phone number that you use in this process, so please use an up-to-date number connected to your active Telegram account.

Telegram for Android

Telegram for WP

Telegram for iPhone / iPad

For more details visit :
https://telegram.org/

CERT-In Vulnerability Note CIVN-2015-0129
Multiple Vulnerabilities in IBM Notes, iNotes and Domino

Original Issue Date:May 18, 2015

Severity Rating: HIGH

Systems Affected

- IBM Notes and Domino 9.0.1 Fix Pack 3 (plus Interim Fixes) and earlier
- IBM Notes and Domino 8.5.3 Fix Pack 6 (plus Interim Fixes) and earlier

Overview

Multiple vulnerabilities have been reported in IBM Notes, iNotes and Domino, which could be exploited by a remote attacker to execute arbitrary code, crash the application, or conduct XSS attacks.

Description

1. Dojo Toolkit Cross-Site Scripting Vulnerability (CVE-2014-8917)

A vulnerability has been reported in IBM Dojo Toolkit in Notes, iNotes and Domino, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute arbitrary code in a victims web browser within the security context of the hosting web site. Successful exploitation could allow the attacker to steal cookie-based authentication credentials and launch other attacks.

For more details visit

http://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2015-0128
http://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2015-1453

CERT-In Vulnerability Note CIVN-2015-0128
Cisco TelePresence Products Command Injection Vulnerability

Original Issue Date:May 18, 2015

Severity Rating: HIGH

Systems Affected

- Cisco TelePresence Advanced Media Gateway Series Software releases prior to 1.1(1.40)
- Cisco TelePresence IP Gateway Series Software
- Cisco TelePresence IP VCR Series Software Releases Prior to 3.0(1.27)
- Cisco TelePresence ISDN Gateway Software releases prior to 2.2(1.94)
- Cisco TelePresence MCU Software releases prior to 4.4(3.54) and prior to 4.5(1.45)
- Cisco TelePresence MSE Supervisor Software releases prior to 2.3(1.38)
- Cisco TelePresence Serial Gateway Series Software releases prior to 1.0(1.42)
- Cisco TelePresence Server Software releases prior to 3.1(1.98) for Hardware release
- Cisco TelePresence Server Software releases prior to 4.1(1.79) for Virtual Machine

Overview

A vulnerability has been reported in web framework of multiple Cisco TelePresence products which could allow a remote authenticated attacker to inject arbitrary commands on the targeted device with root privileges.

Description

This vulnerability occurs due to improper input validation. A remote attacker could exploit this vulnerability by sending a specially crafted parameter value to trigger an input validation flaw in the web framework and execute arbitrary commands on the affected device with the privileges of the root user.

THE TIMES OF INDIA

Tech

Home | Tech | Tech News | Reviews | Jobs | Social | IT Services | Slideshows | How To | Mobiles | PCs | Apps | Gaming | Co

You are here: Home » Tech » Tech News

FOLLOW U

Online dating scams top financial fraud in Australia: Regulator

AFP | May 18, 2015, 12.20 PM IST

READ MORE »Australian Competition And Consumer Commission | online Dating

More than 91,000 scam complaints were received in 2014, figures from the Australian Competition and Consumer Commission (ACCC) showed.

SYDNEY: Australians were tricked out of Aus$82 million (US$66 million) last year, with online dating scams accounting for the biggest losses, the competition regulator has revealed.

More than 91,000 scam complaints were received in 2014, figures from the Australian Competition and Consumer Commission (ACCC) showed.

While losses fell eight percent on the previous year, one tenth of those who reported being targetted were tricked out of more than Aus$10,000 and for 14 people, the losses exceeded Aus$500,000.

ACCC deputy chairman Delia Rickard said most people were reeled in by romance-based cons, with fraudsters making Aus$28 million by tricking people into sending money to a false admirer.

http://timesofindia.indiatimes.com/tech/tech-news/Online-dating-scams-top-financial-fraud-in-Australia-Regulator/article-show/47325743.cms

NDTV GADGETS BETA

HOME | NEWS | REVIEWS | FEATURES | VIDEOS | HUBS | COMPARE MOBILES | TABLET FIN

MOBILES | TABLETS | APPS | GAMING | CAMERAS | TELECOM | SCIENCE | PC/LAPTOPS | HOW TO

YOU ARE HERE: GADGETS HOME > SOCIAL-NETWORKING > SOCIAL-NETWORKING NEWS >

Twitter Harassment Patterns Detailed in WAM Study

Do you feel you are being harassed on Twitter? If yes, you are not alone, a study said.

The study by feminist activist group Women, Action and the Media (WAM) found that, among other things, around a quarter of young men and women have been physically threatened online, and a quarter of young women have been sexually harassed.

WAM got approval from Twitter to accept and submit harassment reports, putting together a picture of who is complaining about accounts or tweets and how Twitter might be able to help, The Verge reported.

WAM focused specifically on 811 harassment reports.

About a quarter of the reports concerned "hate speech" like racist, sexist or homophobic comments, and a slightly smaller number involved releasing private details about individuals.

http://gadgets.ndtv.com/social-networking/news/twitter-harassment-patterns-detailed-in-wam-study-693433

For more details visit
www.infosecawareness.in

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 programming in the application domains of Network Security, e-learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain Management and Wireless Sensor Networks.

Department of Electronics & Information Technology,
Ministry of Comunications & Information Technology,
Government of India

सी डैक
CDAC
www.cdac.in

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

Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)
E-mail : isea@cdac.in

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)