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

InfoSec Newsletter
Nov-Dec 2018

SECURITY OVER WHATSAPP

InfoSec

Ministry of Electronics & Information Technology, Government of India

For Virus Alerts,Incident & Vulnerability Reporting
certin Handling Computer Security Incidents
www.cyberswachhtakendra.gov.in/

सी डैक CDAC
प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

InfoSec Newsletter Nov-Dec 2018

CREDITS

Supported by

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

Message from
E Magesh
Director, C-DAC Hyderabad

Digital Communications has played a pivotal role in improving and increasing the social and work place interactions. The technology has played a great influence and has seen a significant rise in technological application in the area of communications. In fact, people feel more connected while using instant messaging making them spend more time on it, than on any other social media platform like facebook, blogs etc., Today, there are several popular messaging platforms available like wechat, messenger viber, slack & others in usage. Instant messaging provides instant information and instant fun. In many organizations, employees are now collaborating via Instant Messaging (IM), either as a complement to email or as its replacement. WhatsApp helps you stay in touch with friends, share vital information during natural disasters, better connect with families or seek a better life.

One of the very popular instant messaging app is 'WhatsApp' with 1.5 billion monthly active users world wide and 200 million active users in India. WhatsApp provides end-to-end encryption for both private and group conversations so that these cannot be read or manipulated by any third party, even its own creater i.e.,WhatsApp. The ability to go beyond these safeguards could lead to severe breach of privacy. Also the severity of the unchecked spread of fake news is leading to several problems across the country.

The current edition of newsletter will help the readers to understand various security concerns raised over WhatsApp and a few measures that can be taken to avoid them. C-DAC Hyderabad, being the coordinating center for creating mass awareness on Information Security under the purview of ISEA Project Phase II, is glad to release this newsletter on such an important topic, which is of interest for most of the stake holders.

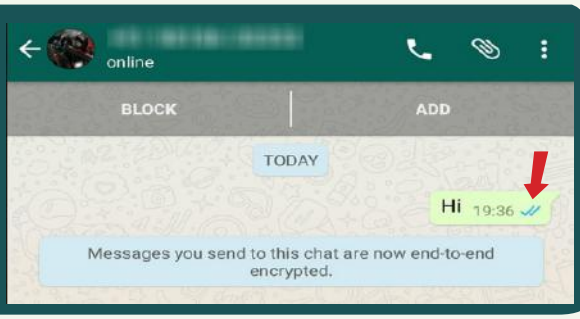
Connect us with /informationsecurityawareness
Follow us at /infosecawa
Subscribe us at /informationsecurityawareness
Follow us at /infosec_awareness

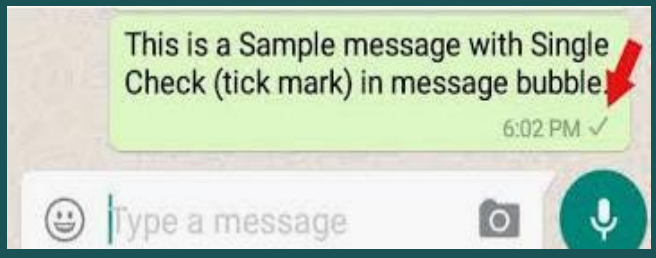
SECURITY OVER WHATSAPP

Instant Messaging Apps are FREE messaging apps available for Android, IOS and all other smart phones. Most of us switched from SMS to instant messaging because of the ease to send and receive messages, calls, photos, videos, documents and Voice Messages. WhatsApp, one of the prominent Instant messaging app which is used by millions in India and all over the world has provided End-to-End encryption in the latest versions of the app to ensure security to the messages. End-to-End encryption ensures only you and the person you are communicating with can read what has been sent, and nobody in between, not even WhatsApp. For added protection, every message you send has its own unique lock and key. Similarly other popular Instant messaging Apps are telegram, wire, signal etc., are commonly used by people.

WhatsApp is a wonderful app, but at the same time it is important to know whether your information and messages on WhatsApp are secure or not. Every message you send in WhatsApp is accompanied by a grey tick indicating the status of the message.

For Instance when you sent a message in WhatsApp you get a notification of two ticks on the bottom of the message indicating that the message is delivered to the recipient. And these ticks turn blue as soon as the message is read by the recipient.





When the recipient mobile is out of coverage area, the message cannot be delivered to the recipient. Then WhatsApp will indicate single tick.

Will End-to-End encryption protects your message before it delivers?

In this newsletter we try to give an insight into

- *Different threats we may face while using WhatsApp and other Instant Messengers*
- *Tips for safe use of WhatsApp*
- *Different example cases of fake WhatsApp messages*
- *Security settings to help you protect yourself.*

Yes, since your message is encrypted with a lock before sent and the key is only with the recipient it will protect your message till the time it delivers. Next question that arises is where are these messages stored till the time these are delivered to the recipient? These messages are stored in WhatsApp server till the time it is delivered and it will be stored there till 30days from the date of the message. **Will end to end encryption secure your message in WhatsApp server?** A skilled hacker can compromise the server. Likewise many issues questioning the WhatsApp and other Instant messenger security and privacy have come up recently.

The fact that it has millions of users makes it a target for hackers who seek to carry out cyber attacks on number of people. The fact that instant messaging has younger generation users will attract online predators. Also anyone in control of a WhatsApp server can add people to a private group with minimal effort. The confidentiality of the group is broken as soon as the uninvited member can obtain all the new messages and read them. With all its positives and negatives WhatsApp has evolved as the most popular messaging service for millions of people all over the world.

Risks that you may come across while using WhatsApp

WhatsApp has strengthened their security over recent years by adding two-step verification and automatic end-to-end encryption but there are still some security threats one should be aware of.

Backups That Are Not Encrypted

The messages you send via WhatsApp are end-to-end encrypted, which means that only your device has the ability to decode them. This prevents your messages being intercepted during transmission, but nothing of these can guarantee safety while on your device. On both iOS and Android it is possible to create a backup of messages to either iCloud or Google Drive. The backups the WhatsApp's creates contains the decrypted messages on your device.

- The backup itself is not encrypted. If someone wanted access to your messages, they would only needthe latest copy of your daily backup.

- It is also vulnerable as there is no ability to change your backup location, meaning that you are at the mercy of the cloud service to keep your data protected.

Therefore, there is no such concept of end-to-end security in the case of an unencrypted backup, which is available on the cloud services; and legal agencies can access with a warrant.

Tip : Since the back ups are not encrypted, It is always better to avoid abusing, bullying through WhatsApp messages and do not forward hoax calls and other threat messages

Web Malware that can compromise your device

- Some attackers created malicious software downloads that would masquerade as WhatsApp Desktop applications. Once installed, these could install and distribute malware or otherwise compromise your computer.

- Others turned to creating websites pretending to offer access to WhatsApp Web. They ask for your phone number in order to "connect you to the service" but in reality it is used to bombard your WhatsApp with spam messages.

Tip : Although WhatsApp does offer a client for both windows and mac, the safest option is to go directly to the source at https://web.whatsapp.com/

Data Sharing between Facebook and WhatsApp

Both Facebook and WhatsApp got together and part of its deal include data sharing from WhatsApp to Facebook. Information like the last time you used WhatsApp and your registered phone number is part of this data sharing between the Facebook/ WhatsApp families.

Tip : Turn off data sharing options on your WhatsApp

Threat to privacy

We share lot of our personal information through WhatsApp knowingly or unknowingly. The main flaw in WhatsApp with respect to privacy is that anyone can add you on WhatsApp if he/she knows your mobile number. For Example any cab driver who called you for assisting the cab service can get hold of your number and add you on his WhatsApp. By adding you, your profile photo, status and "last seen" are visible to general public. All these are at present valuable information for a cyber criminal. Like the Last Seen" status shows when you were online last time.Your status message saying about your holiday gives out the information that you are away from home.

Another critical threat to privacy is due to the fact that WhatsApp is linked with your mobile number. In WhatsApp unique identifier of your account is Mobile No. but it is authenticated only once at the time of registration. When you change your handset without uninstalling WhatsApp then anyone can use WhatsApp linked to your mobile number from old handset. In short, without using your SIM he/she can send messages from your mobile number through old handset.

Tip : Change privacy settings of WhatsApp

Snooping on other WhatsApp User messages

Xnspy, is a monitoring software, which allows users to access target's WhatsApp messenger to all chats, photos and videos exchanged and call logs.

Be aware that detecting the presence of spyware in your cell phone is easy, but detecting these kind of apps is really tough. WhatsApp uses Mac addresses to route messages, which makes it a harder method of sneaking on WhatsApp conversations. By assigning someone else's' Mac address to your phone, you can temporarily intercept their WhatsApp messages.

Tip: The best way to prevent a stranger accessing your WhatsApp is by making sure you never leave your phone lying around, or with someone whom you do not trust. It is better to install tracking software or get a phone's Mac address.

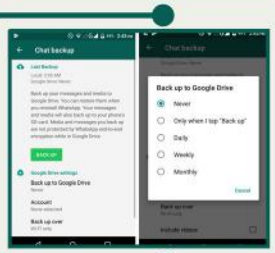
BEHAVIORAL TIPS FOR ALL

- Always be courteous in replying after reading messages.
- Show patience for receiving photos after the party/vacation
- Avoid making fuss over others online behaviour
- Make Appropriate use of Emojis
- Be clear in both words and approach
- Avoid spreading fake news
- Avoid getting into multiple topics at one go
- Do not argue over silly matters
- Never begin a topic that would hurt religious or cultural sentiments.
- Don't spam with unnecessary chains and forward messages
- Control what you see and with whom you interact
- Control what you share

WhatsApp Security Tips

Enable two-factor authentication, to ensure that nobody can set up your WhatsApp without knowing the secret 6-digit code

Make sure cloud backups are off. They are not secured when sharing with the cloud provider



Manage WhatsApp Web effectively, Log out from all computers

Never trust message that claims to come from WhatsApp and demands payment for the service

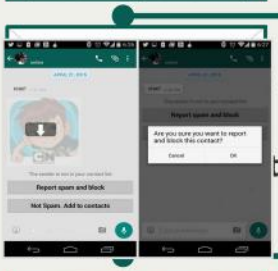
Restrict Access to Your Profile Pic to only contacts.

Avoid using WhatsApp when you are connected to open Wi-Fi networks

Always keep an updated anti virus security solution installed on your mobile device

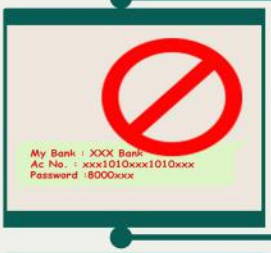
Always read the terms and conditions before downloading any APP

Never accept files or begin downloads from messages sent to you by strangers or unknown numbers



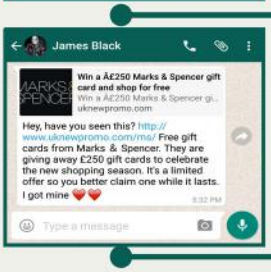
To block an unknown number, open that particular chat window go to more option and block

Never send private information like bank account details, PINs or passwords through WhatsApp

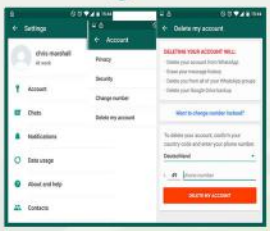


Keep automatic downloads disabled

Never respond to suspicious messages from unknown numbers



Deactivate WhatsApp if you lose your phone



CASE STUDIES

Case 1:

The group admin of a WhatsApp group was arrested from Marathwada, Maharashtra. His crime was being the administrator of a group where a video of a man slaughtering a cow and abusing the Prime Minister was shared leading to circulation of 'objectionable' content. The administrator is the one who creates the group and adds or removes members, so he or she should know who is being added and what content the members may share.

Section153A of IPC deals with 'promoting enmity between different groups on ground of religion, race, place of birth, residence, language etc., and doing acts prejudicial to maintenance of harmony'. Punishment can involve imprisonment ranging from three to five years with fine as well. Section 67 and section 34 of the Information Technology Act (IT Act) also implies to the same case. Section 34: Acts done by several persons in furtherance of common intention. Section 67: Publishing of information which is obscene in electronic form.

If you are a group admin in WhatsApp, regularly have a watch on what content is shared in WhatsApp group that you are admin

Case 2:

There are instances of many cases where a particular fake message is spread in WhatsApp for entertainment; one such attempt was made with our National Anthem. The screenshot of such a message is shown in the figure. It is important to open the link and read/study before you re-tweet, share or like it. Fake stories are designed to mislead you to maximize profit or spread of misinformation. Many a time, rumors makers use shortened URLs and catchy headlines to make it look like the source is a reputed one.

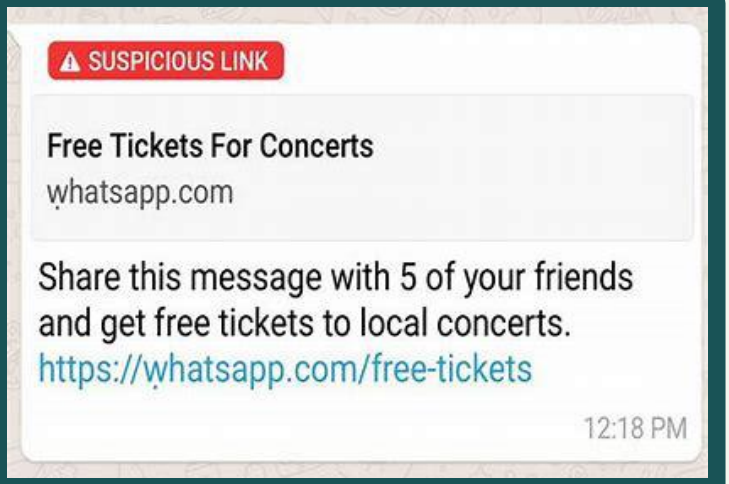
Always read it first. Be thoughtful about what you share

Case 3:

According to research studies it was found that the cognitive psychological profile of people who fall prey to fake news, found that those who apply analytical thinking to what they are reading are less inclined to believe what they are reading. With everything you read or view online, the first step should be to apply your brain and be willing to disbelieve. Even if you read something or watch a video, from dependable sources online, always use your analytical powers to question the intent and honesty of the stories. Here is an example where expensive brands are offered for lower prices.

Be thoughtful about the unbelievable offers that you receive by WhatsApp or in Social media

Case 4:



Even if the article seems to be genuine and is published on a website you trust, with the same fonts and layout, it can still be a fake. The internet is loaded with tools that offer easy templates for people to create fake BBC or New York Times articles. Some websites use similar domain names to confuse readers, with one letter of the alphabet different in the address. A fakeNYT opinion piece on WikiLeaks recently had the URL "opinion-nytimes.com while the real one is "nytimes.com/pages/opinion". Red flags include ".com.co", ".go.com", ".news", ".limo" versions of known media sites

Nothing comes for free, think before you click on unbelievable links

InfoSec CONTEST

InfoSec QUIZ

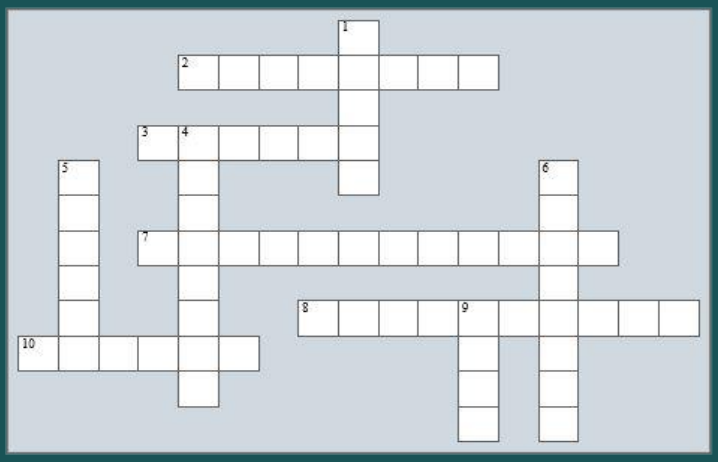
1. Which software can be used as monitoring software, which allows users to access target's WhatsApp messenger to all chats, photos and videos exchanged and call logs.
   a). Xnspy
   b). Popularity
   c). Agentspy
   d). SMS

2. What technology is added in the latest versions of the app to ensure security
   a). Endpoint security
   b). Backdoors
   c). End-to-End encryption
   d). Point to Point Encryption

3. What indication WhatsApp gives you to notify that message is delivered?
   a). Two ticks
   b). One tick
   c). Three tick
   d). No tick

4. How many days will WhatsApp server store the undelivered data?
   a). One day
   b). 20 days
   c). 30 days
   d). Unlimited

5. Will End-to-End encryption protects your message before it delivers?
   a). Yes
   b). No



InfoSec CROSSWORD

Across

2. Avoid spreading
3. The concept of end-to-end security fails in the case of an unencrypted
7. Your _____ is directly linked with WhatsApp that may cause threat to your privacy?
8. When the recipient mobile is out of coverage area, the message cannot be delivered to the recipient. Then WhatsApp will indicate
10. App is the world's 1st Data Recovery Software for Smart phones and Tablets

Down

1. ____ software can be used as monitoring software, which allows users to access target's WhatsApp messenger to all chats, photos and videos exchanged and call logs
4. Line has the feature of ___ your device and PC.
5. While using signal ___ never has access to any of your communication and never stores any of your data.
6. For every message you send in WhatsApp is accompanied by a ____ indicating the status of the message.
9. introduced end-to-end encryption in 2015

Logon to
www.digitalsuraksha.in
www.infosecawareness.in
to participate in
InfoSec Contest and win prizes

INFORMATION SECURITY AWARENESS WORKSHOP

Csit durg@Chhattisgarh

Somerville School@Delhi

Students@Bilaspur

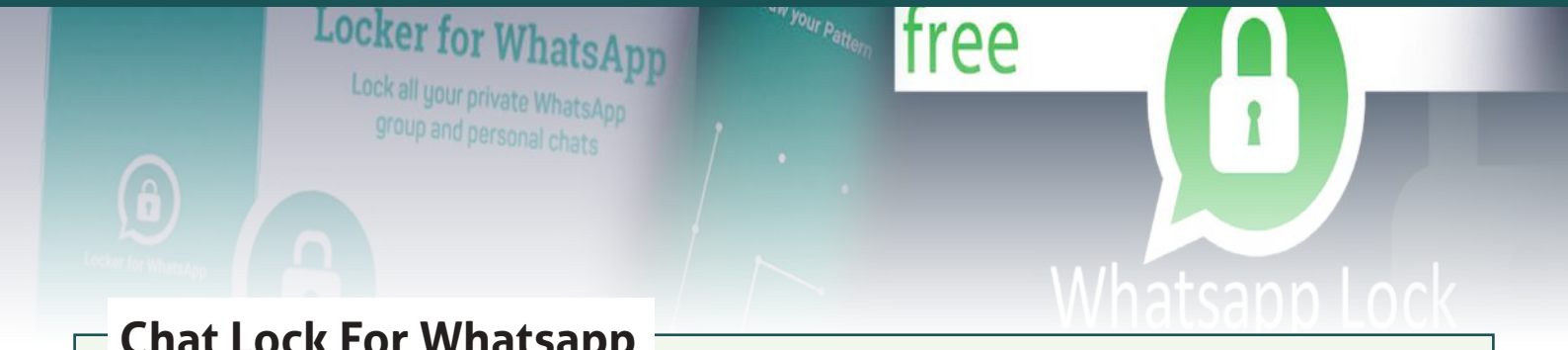
@Rampur Uttar Pradesh

Executive officers, Mazagon dock@Mumbai

Government Girls Degree college@Rampur

Operatives, Mazagon dock@Mumbai

Guru ghasidas central University@Bilaspur



Chat Lock For Whatsapp

By using this app you can easily secure your private and group WhatsApp conversations and maintain their privacy using a pass code. It is free for use. Also one of the best app for locking WhatsApp chats. It can be used to hide your personal chats from others. It supports Fingerprint Authentication. It uses very less space and resources. Design is simple and easy to use interface. Only Minimum permissions required.

https://play.google.com/store/apps/details?id=com.brahmostech.chatlock&hl=en_US

Whatsfile - Hide & secure whatsapp files

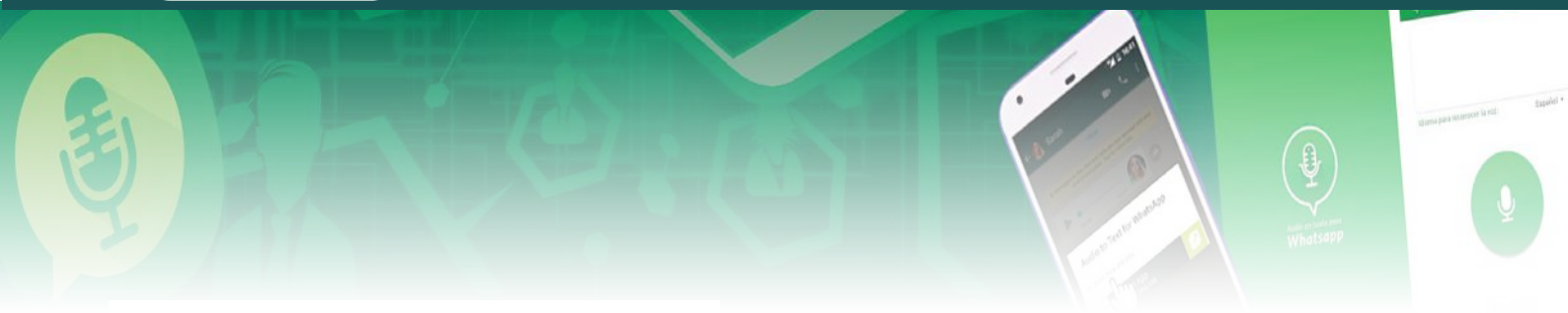
WhatsFile App Smart phone Application helps you to securely hide/delete WhatsApp Images, Videos, Audios and Animated GIFs; WhatsFile App can be used to hide documents before anyone see it. WhatsFile App is a perfect solution to hide/delete media files of WhatsApp in a single click. Hide/delete selected images or videos.

https://play.google.com/store/apps/details?id=com.trigtech.hideone.w

Hide Whats app

This app can help you hide WhatsApp on your phone. The App hidden in it will not be seen on your launcher, recent apps list, app management in system settings and any other app trace on your phone system.You can hide WhatsApp you've already installed. Also erase trace from Recents that is the hidden App will not be shown in 'Recent Apps List'. Hide or mock notifications: The notification can be chosen not to display in the notification bar, or be mocked as other notification content. Set password for it, make your privacy more secure.Cover it as calculator, just you can find it and access your app.

https://play.google.com/store/apps/details?id=com.mediahouselb.whatsfile



Audio to text for WhatsApp

You may have faced a situation where you want to write a WhatsApp message or an SMS and was not be able to write. Thanks to this app you can transcribe your audio to text or message and send it by WhatsApp, SMS, or copy it to use it in any social network. It works in several languages. It is simple and easy to use interface. You can convert your dictation by voice in notes and share it without using WhatsApp keyboard. Audio to text converter for WhatsApp with which you can pass your voice to text and send your messages without writing a single word

https://play.google.com/store/apps/details?id=com.cherry.sttwhatsapp

Dr.fone - Recovery & Transfer wirelessly & Backup

This app is the world's 1st Data Recovery Software for Smart phones and Tablets. It has highest recovery rate in the industry. It can recover photos, videos, contacts, messages, notes, call logs, and more. One of the New feature is that it can easily transfer any files between devices and PC wirelessly. It is free you from cables and client. The only thing you need to do is to open web.drfone. mein a browser.

https://play.google.com/store/apps/details?id=com.wondershare.drfone

Signal

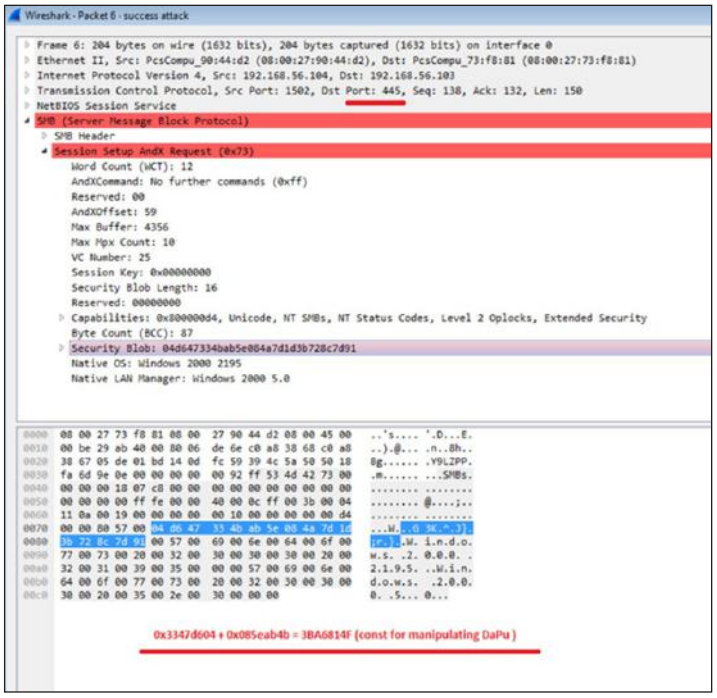
Developed by Open Whisper Systems, Signal is another messaging solution driven by privacy. It uses military-level end-to-end encryption to protect messages, strengthened by an open-source platform that's constantly monitored by its team of developers and improved in its defense systems. Privacy is possible, Signal makes it easy. Using Signal, you can communicate instantly while avoiding SMS fees, create groups so that you can chat in real time with all your friends at once, and share media or attachments with complete privacy. The server never has access to any of your communication and never stores any of your data.

https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms

DARK PULSAR

Dark pulsar is a backdoor which got installed on the victim system through the Eternal Blue exploit, a SMBv1 (Server Message Block 1.0) vulnerability present in Microsoft Operating system. Once this malware reach on victim machine, it opens a backdoor through which other plugin of this malware get loaded onto infected computers. These plugin enhance the functionality of attacker like Responds to a specific ping request of C2 controlled by attacker, load shell code, disable security, enabled the security, payload upload, upgrade implant, run a DLL on the victim machine, Process injection, maintaining persistence and uninstall itself.

Once backdoor fully installed on the victim machine, attacker check its presence by sending the "trans2 SESSION_SETUP" request to the victim machine. Based upon the victim machine response, attacker know that it is infected or not. If a system is found to be infected with this backdoor, then attacker used the SMB as a covert channel to exfiltrate data or launch remote command on the victim machine to perform malicious activity. The port used by attacker for Exfiltrate data from victim machine is not new but the same port used for SMB via 445 as shown in Figure1.



Indicators of Compromise:
MD5:
96f10cfa6ba24c9ecd08aa6d37993fe4

File Location:
%SystemRoot%\System32\sipauth32.tsp

Registry:
HKLM\Software\Microsoft\Windows\
CurrentVersion\Telephony\Providers

Best Practise and Recommendations:
Users are advised to patch their system from Eternal Blue exploit vulnerability having CVE no. CVE-2017-0144with latest patch released by Microsoft from below mentioned link.
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17 -010

Blocks users from connecting to malicious domains, IPs, and URL. Monitor all the outward network connection build by your machine with port no 445..Restrict execution of PowerShell /WSCRIPT in enterprise environment Ensure installation and use of latest version (currently v5.0) of PowerShell, with enhanced logging enabled. Script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

Reference:
https://www .fireeye.com/blog
threatresearch/2016/02/greater_visibilityt.
html

Follow safe practices when browsing the web. Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths. Generally Malware sample drops and executes generally from these locations.

References:
https://securelist.com/darkpulsar/88199/

For more details visit: *https://www.cyberswachhtakendra.gov.in/alerts/DarkPulsar.html*

CERT-In Vulnerability Note CIVN-2018-0189

Uninitialized Stack Memory Usage Vulnerabilities in VMware

Software Affected

- VMware ESXi versions 6.0, 6.5 and 6.7
- VMware Workstation versions 15.x before 15.0.1
- VMware Workstation versions 14.x before 14.1.4
- VMware Fusion versions 11.x before 11.0.1
- VMware Fusion versions 10.x before 10.1.4

Overview

Multiple vulnerabilities have been reported in VMware products which could allow a local attacker on a guest system to execute arbitrary code on the host system or obtain sensitive information.

Description

Remote code execution vulnerability (CVE-2018-6981)
This vulnerability exists in the vmxnet3 virtual network adapter of VMware products due to the use of uninitialized stack memory in the adapter. A local attacker on a guest system could exploit this vulnerability by sending specially crafted requests to the target system.

Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on the host system.

Solution

Apply appropriate patches as suggested by vendor in VMSA-2018-0027

References

VMware
https://www.vmware.com/security/advisories/VMSA-2018-0027.html
Cisco
https://tools.cisco.com/security/center/viewAlert.x?alertId=59115
https://tools.cisco.com/security/center/viewAlert.x?alertId=59116
Security tracker
https://securitytracker.com/id/1042054

CVE Name

CVE-2018-6981
CVE-2018-6982

For more details visit:
https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2018-0189

CERT-In Advisory CIAD-2018-0032

Multiple Vulnerabilities in Apple iOS

Softwares affected

- Apple iOS versions prior to 12.1

Overview

Multiple vulnerabilities have been reported in the different components of Apple iOS which could be exploited by an attacker to cause arbitrary code execution , denial of service (DoS) condition, cross site scripting attacks , gain elevated privilege , read privileged memory and obtain potentially sensitive information on the target system.

Description

The vulnerabilities are due to the memory corruption issues, improper input validation, out-of-bounds read flaw, exploitation of the Miller-Rabin primarily test weakness, restricted files access, privilege escalation flaws, buffer overflow issues, security restrictions bypass and information disclosure flaw.

Successful exploitation of some these vulnerabilities could also allow the attacker to cause user interface spoofing when processing a maliciously crafted mail message.

Solution

Upgrade to Apple iOS version 12.1 Apple Security Advisory
https://support.apple.com/en-us/HT209192

Vendor Information

Apple
https://support.apple.com/en-us/HT209192

References

Apple
https://support.apple.com/en-us/HT209192
Security Tracker
https://securitytracker.com/id/1042003
Center for Internet security
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2018-120/

CVE Name

CVE-2018-4365
CVE-2018-4366
CVE-2018-4367
CVE-2018-4368
CVE-2018-4369
CVE-2018-4371

For more details visit:
https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2018-0032

To share tips / Latest News, mail us to

isea@cdac.in

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events etc.,

About C-DAC

C-DAC established its Hyderabad Centre in the year 1999 to work in Research, Development and Training activities embracing the latest Hardware & Software Technologies. The centre is a Knowledge Centre with the components of Knowledge Creation, Knowledge Dissemination and Knowledge Application to grow in the areas of Research & Development, Training and Business respectively. The R & D areas of the centre are e-Security, Embedded Systems, Ubiquitous Computing, e-Learning and ICT for Rural Development. The centre has developed over a period of time a number of products and solutions and has established a number of labs in cutting edge technologies. In line with these R&D strengths, the centre also offers Post Graduate level diploma courses. Centre is also actively involved in organizing faculty training programs. The centre regularly conducts skill based training and information security awareness programmes.

BOOK POST

For queries on Information security

Call us on Toll Free No.

1800 425 6235

between 10.00 AM to 6.00 PM
or give us a missed call
we will call you back within 24 hrs

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

Between 9.00 AM to 5.30 PM

Subscribe us on

https://www.youtube.com/c/InformationSecurityEducationandAwareness

Follow us on

https://twitter.com/InfoSecAwa

Connect us with

https://www.facebook.com/infosecawareness

Ministry of Electronics and Information Technology (MeitY)
Government of India

सी-डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 501510, Telangana(India)
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)