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

InfoSec Newsletter

JULY-AUGUST 2019

SECURITY AWARENESS ON WEARABLE GADGETS

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
Plot No: 6&7, Hardware Park Sy. No.1/1, Srisailam Highway Raviryal (V & GP), Via Ragaanna guda, Maheshwaram (M), Ranga Reddy District, Hyderabad - 501510Telangana(India)
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)

InfoSec Newsletter Jan-Feb 2019

CREDITS

Supported by

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

Message from
E Magesh
Director, C-DAC Hyderabad

Modern Technology has revolutionized our lives by creating useful resources that simplify every activity of our daily life and put useful information at our fingertips. These amazing innovations in technology have infiltrated our lives and have become so prevalent that they have become a part of every moment of our life. It has further extended its presence in everyday life by being part of our human body through Wearable gadgets that simply enhance our life.

These gadgets have moved from niche to mainstream over the last two years. A big leap took place for wearable technology with google glass in 2013.Wearable devices market is projected to gain significantly during estimated period of 2018-2023, on account of trends like rising fitness trends, lifestyle modernization, growing keenness to own sophisticated devices and surging internet penetration. Considering the amount of sensitive information that is held within wearable gadgets, commonly used by individuals, there is a need to create awareness about the security and privacy constraints that has to be followed. Every user of wearable technologies has a responsibility to use them appropriately and to consider the privacy of others when using them in public.

The current edition of newsletter on *Security Awareness on Wearable gadgets* educates the reader with the cyber security issues and concerns that can affect the businesses and individuals and a few case studies. Hope this newsletter helps in creating awareness and at the same time sensitize people regarding the cyber security aspects related to the wearable gadgets.

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

InfoSec CONCEPT

SECURITY AWARENESS ON WEARABLE GADGETS

Wearable gadgets are rapidly invading our home and office space in the same way how smartphones did. The wearables currently in use are smart watches, smart glasses, hearables, fitness and health trackers, smart jewelry and smart clothing. The popularity of these devices is growing rapidly all around the world. These devices offer convenient and fun platforms with displaying notifications, controlling media libraries, or accessing personal verbal assistants, track workouts, check emails, etc., A few to mention are Apple Watch, Pebble Watch, Microsoft Band, Fitbit, Jawbone Up, Nike+ Sportband, Motiv Ring tracks fitness activity, heart rate, and sleep patterns in a slim, minimalist ring and medical wearables, like iHealth's wireless pulse oximeter and Withing's blood pressure monitor etc.,

Gartner, Inc. forecasts that worldwide shipments of wearable devices will reach 225 million in 2019, an increase of 25.8 percent from 2018. End-user spending on wearable devices is forecast to reach $42 billion in 2019. Of that, $16.2 billion will be on smartwatches. With the immense popularity most consumers ought to buy these devices don't think much about security risks involved while using these devices. These wearable gadgets in a way help cyber criminals by acting as another way to hack user accounts, enabling them to steal sensitive personal information, or even money from their financial accounts. Most of the end users of wearable gadgets have a perception that, because it is coupled to a smartphone the security is already built-in, but in reality that is not the case.

These devices collect data about the user and communicate with a base station, which in most cases is the user's phone. Many of the devices available to consumers are able to go way beyond their primary function – e.g., the more expensive fitness trackers also monitor vital signs and offer email and Internet connectivity. The same is true for smart watches that also allow users to pay for goods and services. It's not hard to see how the Internet of things – the connectivity that links an employee's watch to a personal mobile device that in turn has access to a company's network where sensitive financial and customer information is stored – suddenly becomes a cyber-security nightmare. With all this it is important that security needs to be built-in to the wearable devices.

History of Wearable devices

Wearable technology has taken off in a host of directions once considered impossible. The device landscape has come a long way from the earliest wrist-sized calculators or the first Bluetooth headsets. Pulsar's Calculator Wristwatch can be considered as the first consumer wearable device to achieve global success. In 2000, the first Bluetooth headset was sold and in 2004, the first GoPro was launched. Google Glass or simply called as Glass, released in 2013, was the first voice-operated optical head-mounted display product to combine hands-free internet access with augmented reality and the ability to capture images This is considered as the first wearable device that kick start the growth of Wearable gadgets. Glass is an eyewear device that has built-in computer in the frame of a pair of glasses. It provides numerous innovative features that make people life more fun. However, many concerns have been raised from various sources regarding to some issues that could be threatened wearer's security and privacy. The most successful wearable devices on the market right now are smart watches and health and fitness tracker.

What Is Wearable Technology?

Wearable technology has changed the way we receive, use, and share data. There is a fundamental paradigm shift in how we view and interact with technology. Wearable technology is a category of electronic devices that can be worn as accessories, embedded in clothing, implanted in the user's body, or even tattooed on the skin. The devices are hands-free gadgets with practical uses, powered by microprocessors and enhanced with the ability to send and receive data via the Internet.

Types of Wearable Gadgets

Wearables comprise four main categories: smart glasses and headgear, smart watches, wearable medical devices and fitness trackers. All of these have three enabling technologies that make them 'smart':"

- Sense and translate data;
- Collect and prepare data for transmission; and/or
- Transmit data to off-site storage for processing and reporting.

Sensors

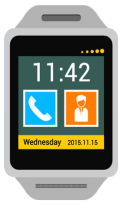
Sensors that capture impulses from the user's body or surroundings, which they translate into actionable data

Microprocessors

Microprocessors that extract, transform and load the data into a transmittable format

Transmitters

Transmitters that wirelessly send the data to a cloud storage for further processing and reporting

Smart glasses and headgear	Fitness trackers	Smart watches	Wearable medical devices	Smart clothing and accessories
e.g.Google glasses and Samsung's Gear VR	e.g.Fitbit, Nike FuelBand, and Microsoft Band	e.g. Apple and Android watches	e.g.Medtronic Continuous Glucose monitoring system and the ZIO Wireless Patch	e.g.Visijax products, Levi's Smart Jacket
				

Are there security concerns with wearables?

The increase in the number of applications available for smartwatches will create new opportunities for fraudsters to compromise wearable devices for access to highly valuable personal information.

Many wearable products are able to track more than the simple information for which they are marketed. Two examples of this include:

- High-end fitness trackers that can track not only steps but other health vitals and even offer email and social media functionality and connectivity; and
- Smart watches that offer mobile payment functionality via transmission (e.g. paying for your Starbucks without lugging around your wallet).

Wearable Technology Security Issues

The risks posed by wearables are broadly classified into three "classes":

- Cyber;
- Bodily injury; and
- Technology errors and omissions

Each risk class poses its own problems the following sections will look at the business risks list approaches to minimize those risks. Wearables linked to mobile devices, which are in turn linked to a corporate network can put organizations to risks of attack. Even though the wearable itself may not be the primary target of an attack, its link to a mobile device creates another point of entry for cybercriminals to exploit, especially since wearables security is a relatively a new frontier. Information that can be stolen and exploited includes real-time geolocation information, emails, contacts, and other proprietary information on the device.

Wearable technology security issues to businesses:

Signal interception

An employee brings his own smart glasses to work, which is connected to his smartphone. His phone, in turn, is connected to a company network where sensitive data is stored. A thief can intercept the Bluetooth from the smart glasses display to a cloud data store and steal sensitive data.

Corporate espionage

An executive enters his building wearing a wireless identity authenticator. A similarly dressed corporate spy can enter a few steps behind him armed with a wireless signal interceptor. After capturing the executive's unencrypted PIN number from the electronic signature, the spy can now move about the building with all the permissions the executive enjoys, including access to intellectual property, which he can then sell to competitors.

No Regulation or Compliance

Companies who suffer a data breach that breaks compliance or regulatory requirements for their specific industry will not be able to blame on the wearables. They will still be held fully accountable. Ignorance of wearable device security and manufacturer or third-party app policy is of no way to defense.

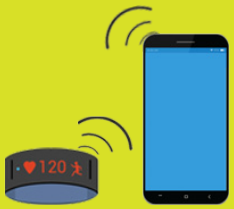
Wearable technology security issues for consumers

From simple fitness trackers that connect to a mobile phone, to stand-alone smartwatches, potentially sensitive personal and sometimes financial information is being passed to the app and to the manufacturer. Users may be asked for access to their files, location, contacts, camera and personal information (age, height, weight, and gender).

- **Easy Physical Access to Data:** The fact that many wearables store data on the local device without encryption is a real issue. There is often no PIN or password protection, no biometric security and no user authentication required to access data on a wearable. If it falls into the wrong hands, there is a risk that sensitive data could be accessed very easily.

- Ability to Capture Photos, Videos and Audio: It is easy for someone to take photographs or record video or audio files using something like a smartwatch or smart glasses. Secret capture of confidential information, and videos and images of sensitive data, is a very real possibility.

- Insecure Wireless Connectivity: The fact that wearable devices tend to connect to our smartphones or tablets wirelessly using protocols such as Bluetooth, NFC and Wi-Fi creates another potential point of entry. We may have Bluetooth on our smartphones turned on all the time. Many of these wireless communications are insufficiently secure to guard against a determined brute-force attack.



- Lack of Encryption: Some third-party apps neglect basic security standards and send or store information that is not encrypted. The kind of data that is automatically being collected by wearables is very valuable to the right people.

- Patching and Vulnerabilities: Many wearables run their own operating system and applications. The same principles that apply to keeping the software on your desktops, laptops, smartphones and tablets fully patched and up to date to avoid the latest vulnerabilities also apply to wearables.

To minimize wearable technology security issues, businesses should look for the following features in the wearables they allow and, if they cannot find them, they should demand them from manufacturers:

- **Custom security levels:** give users the ability to choose the security level they are comfortable with when they install their device or pair it with their smartphone. Users seldom consider security when wearing their devices, so defaulting to the least secure settings opens vulnerability for hackers to exploit.

- **Remote erase feature:** enable wearable users to remotely erase and/or disable their device if it is ever lost or stolen. Wearable device manufacturers should consider offering the same feature.

- **Bluetooth encryption:** Bluetooth offers an encryption API when exchanging data between a device and its target data store, but few companies take advantage of it because it decreases battery life.

- **Encryption of critical data elements:** the most critical pieces of data transferred between wearable devices and data stores are user IDs, passwords, and PIN numbers. Incredibly, most wearable devices transmit these data elements in plain text with no encryption at all.

- **Cloud security:** data is often transmitted from a wearable device to a smartphone and then to a cloud data store. Virtualized clouds can secure data with multiple diverse operating systems, each operating within a different security context. Wearables manufacturing companies should consider similar functionality and your business should demand it.

Example cases:

- **Ecommerce site shutdown:** a smart watch user connects to a company network. The smart watch is infected with malware, due to vulnerability in the device software. The malware infects the corporation's network, executing a DDOS attack, shutting down the company's e-commerce system for two days.

- **Virtual reality device software failure:** a trucking company contracts with a training company that uses wearable virtual reality devices to train long haul truckers for their Commercial Driver's License (CDL) certification. A glitch in the device software prevents completion of the CDL program, resulting in the trucking company not having an adequate number of drivers. The trucking company fails to complete shipping contracts, losing revenue and customers. Additionally, the training company suffers damage to reputation and a loss of business.

The security challenge with wearable devices is by no means undefeatable, and the wearable trend will undoubtedly be a real boon, but it is important to treat it more seriously. There are several simple steps that users can take to ensure security:

- Opt-in only for the information required for use of the app.
- Leverage the highest level of security offered, such as biometrics.
- Practice good password hygiene if passwords must be used, including not reusing passwords across multiple applications and changing passwords periodically.
- Be knowledgeable about phishing attempts to get information from those appearing as their manufacturer.
- Don't click on links in emails or texts unless you are sure they are from a trustworthy source.
- Download software updates when they are available

References

1. *https://securitytoday.com/Articles/2018/07/30/Wearables-Open-Door-to-Many-Security-Vulnerabilities.aspx?Page=4*
2. *https://smallbiztrends.com/2016/02/wearable-technology-security-issues.html*
3. *https://www.condley.com/accounting-edge/wearable-technology-cyber-security-threat/*
4. *https://www.researchgate.net/publication/303870892_Wearable_Technology_Devices_Security_and_Privacy_Vulnerability_Analysis*
5. *https://www.statista.com/topics/1556/wearable-technology/*
6. *https://www.csoonline.com/article/3054584/7-potential-security-concerns-for-wearables.html*
7. *https://www.smartinsights.com/digital-marketing-strategy/wearables-statistics-2017/*

INFORMATION SECURITY AWARENESS WORKSHOP

Excel school, Guwahathi

HPCL, Visakhapatnam

ISEA Awareness for CISF Officers, Guwahathi

Mazagon Dock Shipbuilders Limited, Mumbai

Awareness for the children during Summer Camp organised by Rachakonda Police dept

ISEA awareness workshop to CRPF senior officers at CRPF, headquarters , Delhi

ISEA awareness@Vizag Steel Plant

ISEA awareness@CISF Chennai

InfoSec VIRUS ALERTS

ANDROID MONOKLE MALWARE

A new mobile remote access trojan (RAT) for Android called Monokle, has been reported using novel techniques to exfiltrate data. Monokle uses a range of intrusive capabilities to conduct various types of cyber attacks. The trojan is distributed to targets via fake apps camouflaged as genuine apps such as Google Play, Skype, UC Browser, Pornhub, etc

So far Monokle is directed only against Android devices. The researchers found several references to a planned iOS version, including unused commands and data transfer objects in its source code. Typically,victims are infected when they download trojanised versions of what appear to be legitimate Android applications that otherwise operate as intended..

The attacker can use Monokle to steal the following information:

- It has the ability to self-sign trusted certificates to intercept encrypted SSL traffic and does not require any root access to exfiltrate data.
- A phone's lockscreen activity can be used to obtain passwords to steal personal information as well as gain access to third party apps

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

CERT-In Vulnerability Note CIVN-2019-0130
Linux Kernel net/ipv6/ip6mr.c Code Execution Vulnerability

Overview
A vulnerability has been reported in the Linux kernel's net/ipv6/ip6mr.c function which could allow an attacker to control a pointer in kernel land and execute arbitrary code on a targeted system.

Description
This vulnerability exists in net/ipv6/ip6mr.c in the Linux kernel due to insufficient checks on the sk_type and protocol in the ip_mroute_setsockopt() and ip_mroute getsockopt() functions. An attacker could exploit this vulnerability by setting a specific socket option on the targeted system.

Successful exploitation of this vulnerability could allow an attacker to control a pointer in kernel land and cause an inet_csk_listen_stop general protection fault, or potentially execute arbitrary code under certain circumstances.

Solution
Apply appropriate patches as mentioned in the below link
https://www.kernel.org

For more details visit:
https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2019-0130BVNOTES01&VLCODE=CIVN-2019-0034

CERT-In Vulnerability Note CIVN-2019-0129
Multiple Vulnerabilities in Adobe Acrobat and Reader

Overview
Multiple vulnerabilities have been reported in Adobe Acrobat and Adobe Reader which could allow an attacker to execute arbitrary code and obtain sensitive information on the targeted system.

Description
These vulnerabilities are caused due to various errors in the affected software namely Out-of-Bounds Read, Out-of-Bounds Write, Command Injection, Use after Free, heap-overflow, Buffer error, Double Free, Integer Overflow, Internal IP Disclosure, Type Confusion and Untrusted Pointer Dereference.

Successful exploitation of these vulnerabilities could allow the attacker to execute arbitrary code on the targeted system.

Solution
Apply appropriate updates as mentioned:
https://helpx.adobe.com/security/products/acrobat/apsb19-41.html

For more details visit:
https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2019-0129

InfoSec QUIZ

1. Gartner, Inc. forecasts that worldwide shipments of wearable devices will reach _____million in 2019
   a). 422 b). 100
   c). 225 d). 220

2. Glass is an _____ device that has built-in computer in the frame of a pair of glasses.
   a). Ear wear b). Hand wear
   c). Eye wear d). None of the above

3. Wearable gadgets collect data about the user and communicate with a base station, which in most cases is the user's _____.
   a).Wi-Fi b). email
   c). office d). Phone

4. Which year the first Bluetooth headset was sold?
   a).2004 b).2000
   c).1995 d).2019

5. _____was the first voice-operated optical head-mounted display product to combine hands-free internet access with augmented reality and the ability to capture images
   a).Apple watch b).Glass
   c).Fitbit d).Bluetooth head set

6. High-end fitness trackers that can track not only steps but other _____ and even offer email and social media functionality and connectivity
   a).Health vitals b).Finance
   c).All the above d).None of the above.

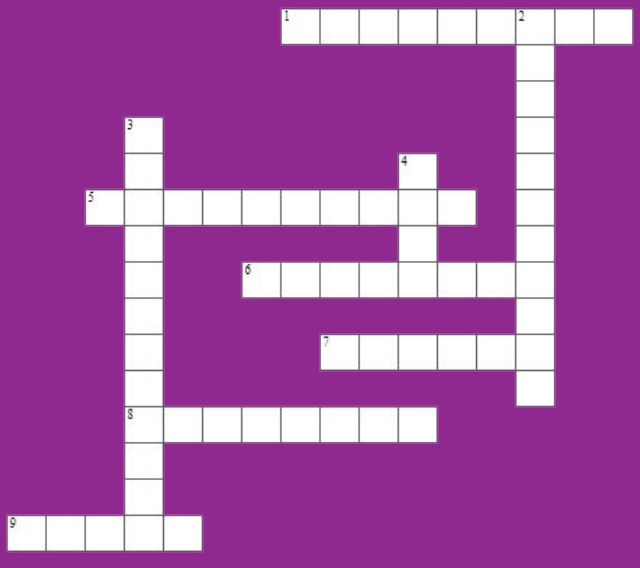
InfoSec CROSSWORD

Across

1. End-user spending on wearable devices is forecast to reach $_____ billion in 2019.and connectivity
5. Pulsar's _____ Wristwatch can be considered as the first consumer wearable device to achieve global success.
6. Wearable gadgets are hands-free gadgets with practical uses, powered by microprocessors and enhanced with the ability to send and receive data via the _____.
7. Wearables linked to _____devices, which are in turn linked to a corporate network can put organizations to risks of attack.
8. Glass is an eyewear device that has built-in _____in the frame of a pair of glasses.
9. _____is considered as the first wearable devices that kick start the growth of Wearable gadgets.

Down

2. _____extract, transform and load the data into transmittable format.
3. The most successful wearable devices on the market right now are _____ and health and fitness tracker.
4. Wearables comprise _____main categories



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

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)