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

InfoSec Newsletter

Jan-Feb 2019

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

Honorary Professor. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team
Ch A S Murty
K Indra Veni
K Indra Keerthi
P S S Bharadwaj

Action Group Members
HoD (HRD), MeitY
Shri.Sitaram Chamarthy (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, MeitY

Compiled by
E Magesh, Director
G V Raghunathan
Ch A S Murty
M Jagadish babu

From C-DAC
E Magesh, Director

Acknowledgement
HRD Division
Ministry of Electronics &
Information Technology

Supported by

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

Message from
E Magesh
Director, C-DAC Hyderabad

The Internet of Things (IoT) refers to inter connected devices connected through the internet that are able to collect and exchange data. Growing need for real-time monitoring, tracking and automation coupled with favorable government initiatives like smart cities, smart transportation, smart grids etc., has paved way for the bloom of Internet of Things (IoT) in India. IoT market in India is projected to grow more than 28% by 2020 and is also expected to propel the use of IoT technology in the country over the next five years.

As the number of connected devices increases it also leads to exploitation of safety vulnerabilities present in IoT devices which are varying in standards. Because of the ability of the devices to connect to the internet and their widespread usage, IoT products are prime targets for cyber criminals as they take advantage of lack of adequate protections. The security challenges with respect to Internet of things are not known to most of the people who use it. Also most of them are hardly aware of extent of impact that a security breach on IoT can cause to an individual. It has now become a necessity to ensure security for IoT devices.

The Newsletter 'IoT Security', is an effort in this direction by C-DAC, to create awareness on the need of Internet of Things and at the same time sensitize people regarding Common cyber-attacks that effect IoT devices, Challenges in IoT and a few Case Studies. Hope this Newsletter will help in creating awareness about the challenges and issues of Internet connected world.

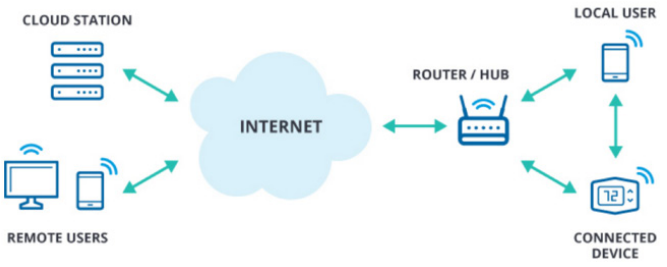
Connect us with /informationsecurityawareness
Follow us at /infosecawa
Subscribe us at /informationsecurityawareness
Follow us at /infosec_awareness

IoT

"The Internet of Things: Challenges and Issues of an Internet connected world"

The Internet of Things, also termed as IoT, is nothing but everyday devices connected to Internet. These devices hold the capability of doing tasks with or without human interaction. Devices like doorbells, home lighting system, toys, water heaters, air conditioners or any device in our day to day life can be a part of this connected system. These connected devices help in making our life easier. For example, lights at home activate automatically when your phone recognizes, that you are close to home. IoT devices can be used for multiple purposes but they are most commonly used in daily automation devices. These devices function by collecting data from sensors and then either store the data locally or send the data to the cloud via the internet or process the data and internally send commands to other devices for further action.

The IoT market is growing at an amazing pace and more and more people started using IoT. New devices are added to the IoT market regularly making it more and more popular. With the rapid growth of communication and internet technology, our daily life routines are more relying on a virtual world. The IoT has a major role in integrating the virtual world and the real world on the same platform. IoT has gradually spread to all aspects of human life, such as education, healthcare, business, involving the storage of sensitive information about individuals and companies, financial data transactions, product development and marketing. However, like any other device, IoT devices also have their own individual security issues.



https://www.whitehatsec.com/blog/a-model-for-successful-iot-security-assessment/

IoT devices collect sensitive information which makes these devices potential targets for attacks. Security aspect was not considered by designers while designing IoT devices. But as popularity of IoT increased, attackers also realized that it is much easy to break into these devices without using much of an effort. Threats on IoT are seen to be increasing on daily basis; and attacks have been on the increase in both numbers and complexity. The tools available to cyber criminals are becoming more sophisticated, efficient and effective. As an example, a pacemaker is a device responsible to regulate the function of the heart.

Pace maker uses this vital data and directly take action on a human body. With just a few malicious commands an attacker can even cause death. With all this it creates a need for creating awareness on how insecure IoT devices are and why it is important to secure these devices.

Need of Internet of Things

- Increase in internet users have led to the popularity of IoT devices.
- Using Internet of Things, connection cost can be decreased by Wi-fi connections, built-in sensors in devices and also by maximum number of devices connected together by a common medium.
- Through Internet of Things, internet connectivity can be extended beyond traditional devices like desktop and laptop computers, smart-phones and tablets to a diverse range of devices including connected vehicles, home automation/smart home, wearable devices, connected health care devices, and appliances with remote monitoring capabilities.

IOT devices: Example

Humans	Home	Retails	Industry	Office	Vehicles
wearable devices	home controllers	Self-checkouts	equipment optimization	energy management	real-time routing
in-body devices	security systems	Inventory optimization	health and safety	productivity	traffic control
health and wellness		operation efficiency	construction	autonomous vehicles	maintenance

The connected devices or machines are potential target for cybercriminals for several reasons:

1. Most IoT devices are operated without human presence, thus it is easy for a cybercriminal to physically gain access to them.
2. Most IoT components communicate over wireless networks where a cybercriminal could obtain confidential information by using the technique called 'eavesdropping'.
3. Most IoT components cannot support complex security schemes due to low power and less resource with respect to computing capabilities

For example: Attacks on home automation systems and taking control of heating systems, air conditioning, lighting and physical security systems. The information collected from sensors embedded in heating or lighting systems could inform the intruder when somebody is at home or not.

Common cyber-attacks that effect IoT devices are:

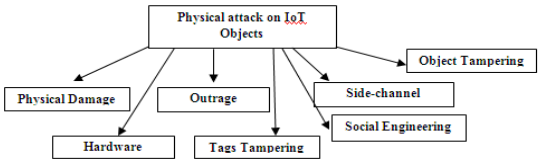
The IoT is facing various types of attacks. These are active attacks and passive attacks that may easily disturb the functionality and abolish the benefits of its services. In a passive attack, an intruder just senses the node or may steal the information but he never attacks physically. However, the active attacks disturb the performance physically. These active attacks are classified into two further categories that are internal attacks and external attacks. Such vulnerable attacks can prevent the devices to communicate smartly. Hence, the security constraints must be applied to prevent devices from malicious attacks.

Different levels of attacks are categorized into four types according to their behavior propose and possible solutions to threats/attacks.

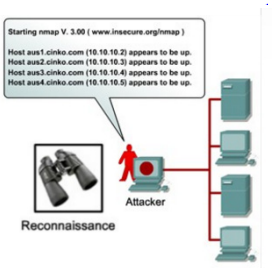
1. Low-level attack: If an attacker tries to attack a network and his attack is not successful.
2. Medium-level attack: If an attacker/intruder or an eavesdropper is just listening to the medium, but do not alter the integrity of data.
3. High-level attack: If an attack is carried on a network and it alters the integrity of data or modifies the data.
4. Extremely High-level attack: If an intruder/attacker attacks on a network by gaining unauthorized access and performing an illegal operation, making the network unavailable, sending bulk messages, or jamming network.

Different types of attack, nature/behavior of attack are discussed in this section.

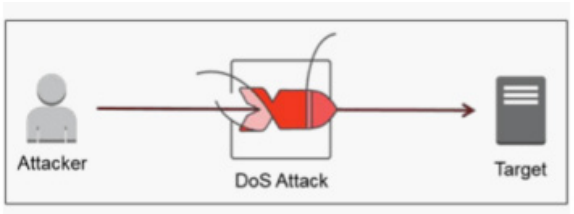
1. **Physical attacks:** This sort of attack is tampering the hardware components. Due to the distributed nature of the IoT, most devices typically operate in outdoor environments, which are highly susceptible to physical attacks.



2. **Reconnaissance attacks:** This mainly accounts for unauthorized discovery and mapping of systems, services, or vulnerabilities. Examples of reconnaissance attacks are scanning network ports, packet sniffers, traffic analysis, and sending queries about IP address information.



3. **Denial-of-service (DoS):** This kind of attack is an attempt to make a machine or network resource unavailable to its intended users. Due to low memory capabilities and limited computation resources, majority of devices in IoT are vulnerable to resources being used by attackers.



4. **Access attacks:** In this unauthorized persons gain access to networks or devices to which they have no right to access. There are two different types of access attack: the first is physical access, whereby the intruder can gain access to a physical device. The second is remote access, which is done to IP-connected devices.

5. **Attacks on privacy:** Privacy protection in IoT has become increasingly challenging due to large volumes of information easily available through remote access mechanisms. The most common attacks on user privacy are:
   - **Data mining** enables attackers to discover information that cannot be obtained from databases.
   - **Cyber espionage** using cracking techniques and malicious software to spy or obtain secret information of individuals, organizations or the government.
   - Eavesdropping is listening to a conversation between two parties
   - **Tracking** a user's movement can be tracked by the devices unique identification number (UID). This may result in tracking a user's location facilities or identifying them in situations in which they wish to remain anonymous.
   - **Password-based attacks:** attempts are made by intruders to duplicate a valid user password. This attempt can be made in two different ways:

   1. Dictionary attack – trying possible combinations of letters and numbers to guess user passwords;
   2. Brute force attacks – using cracking tools to try all possible combinations of passwords to uncover valid passwords.

6. **Supervisory Control and Data Acquisition (SCADA) Attacks:** As any other TCP/IP systems, the SCADA system is vulnerable to many cyber-attacks. The system can be attacked in any of the following ways:
   i. Using denial-of-service to shut down the system.
   ii. Using Trojans or viruses to take control of the system.

Examples to illustrate extent of risk because of IoT

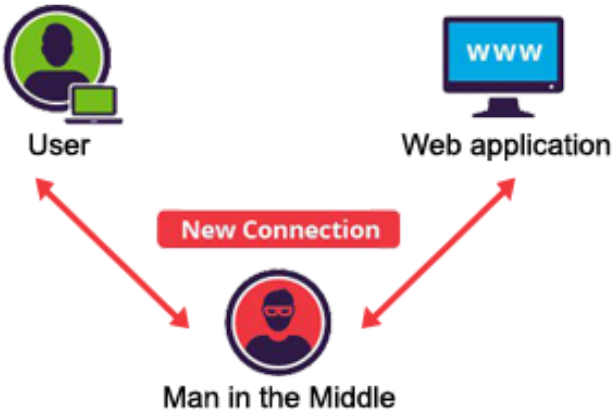
Remote Access of phone through Apps

Unauthorized app stores act as a potential target for hackers togain full control of a victim's phone. For this they need to add their infected (unofficial) version of the app into the Google Play Store. This will not help the victim to keep malware away. An example for this is the online game termed 'Pokemon Go', which has a version known as 'wannabe'. This version will allow remote access to tools such as DroidJack (also known as SandroRAT) into the Google Play Store. DroidJack is a malware that specifically targets Android users and once it is installed in your phone it can access everything on the device. Once the hacker is successful in installing the unofficial version, the hacker can hack the user's data like email, contact, photos, videos, text messages or even the user's device camera or microphone and also to an extent of accessing Google's location data. This happens when apps are downloaded from unofficial play store.

Critical Infrastructures -Data Theft

Cyber-attacks against critical infrastructures are referred to as "nightmare scenarios". Because critical infrastructures depend on giant IT networks, that incorporate IoT devices. They require cyber defenses that are just as powerful and large as they are. It is found that there is a tremendous increase in cyber-attacks reported on IoT devices. One such cyberattack on critical infrastructures was Operation Dust Storm, a multi-year, multi-attack campaign against companies in Japan, South Korea, U.S. and Europe. Different targets included: electric utilities, oil and gas, finance, transportation and construction. The attack methods included: spear phishing, waterholes, unique backdoors, zero-day variants etc...

Smart Devices - Man-In-The-Middle Attacks



SSL vulnerability was recently found on a line of a Smart Fridges, in a penetration test that was part of an IoT hacking challenge. The inter-connected fridge is programmed to download Gmail Calendar information to an on-screen display causing threat to Google credentials of the smart fridge user. The smart fridge runs Google calendar so that its user can manage and view events from the fridge screen. In this case the weakness lies in its failure to validate SSL certificates -- enabling man-in-the-middle attacks between the fridge and Google's servers. Because the Gmail calendars on the smart fridge are downloaded from Google's server, itbecomes a beneficial attack point for cyber criminals to gain user credentials.

Other vulnerabilities were also found in such systems like firmware attacks (a fake firmware update), TCP services and certificate challenges (found in the smart fridge's mobile app code).

Webcams - Remote Access Trojans

Webcams are vulnerable to remote access hacks, even the small cameras we have on our laptop screens are vulnerable. These are often main points of attack for cyber criminals, as they can be an easy way to steal sensitive corporate data or even spying on kids. Once cyber criminals manage to install a malware on a device, they can turn on the infected computer's camera and record or take a screenshotof what is going on. Many people have raised security threat behind webcams. In addition to spying on users, hackers can send malicious emails on behalf of the hacked computers owner orlaunch a massive attack to harm other computersin the name of the hacked user credentials.

Commercial Aircrafts - DDoS and Botnets

The aviation industry is a favorite target for cyber criminals, orin other words, a privileged target for hackers who are interested in the intellectual property of many companies in the sector.

Remote hijacking

Security flaws in communication technologies utilized in the aviation industry enables hackers to remotely attack/control in flight and on-board systems. A hacker has demonstratedhow the flight management system (FMS) could be attacked, which can open a gateway for cyber criminals to attack other critical systems such as flight controls, engine and fuel systems, navigation receivers, surveillance systems, aircraft displays, and others. It was reported that a hacker could hackan aircraft, (and was able to do so 20 times during one flight) and overwrite the code on the plane's "Thrust Management Computer" while it was on air, allowing him to monitor traffic from the cockpit system. He could also issue a climb command and could make the plane briefly change its course.

Jamming attacks:

Hackers could also flood flight management systems which control the takeoff and landing of all flights with a network of botnets and cause the platform to crash. The attacker injects a ghost flight into the air traffic control system to alter the projection and mapping of airplanes, or delete their position from the radar screen.The attackcan have dire consequences as the hackers compromise the accuracy of data provided to the aircraft management, such as speed, location and direction of nearby airports and other planes.

Distributed-denial-of-service (DDoS) attacks have grown in popularity to carry out a range of malware injection activities. Within such attacks, hackers utilize botnets of compromised networks to flood air traffic control and other critical systems with traffic, which results in a crash of the platform. Attackers may also ask for a ransom amount from the authorities to prevent disruption of flight management and control systems.

Challenges in IoT

The security concern is the biggest challenge in IoT now. The application data of IoT could be industrial, enterprise, consumer or personal. This application data should be secured and must remain confidential against theft and tampering. For example, the IoT applications may store the results of a patient's health or shopping store. The IoT is meant to improve the communication between devices but still, there are issues related to the scalability, availability and response time. Security is a concern where the data is securely transmitted over the internet. Among different security challenges, the most important challenges relevant to IoT are discussed below.

1. ***Data Privacy:*** Some manufacturers of smart TVs collect data about their customers to analyze their viewing habits. So the smart TVs have a challenge of securing data privacy of the user during transmission.

2. ***Data Security:*** Data security is also a great challenge. While transmitting data seamlessly,

it is important to hide from other observing devices on the internet.

3. ***Insurance Concerns:*** The insurance companies may be able to collect data from IoT devices on vehicles about health, contact details on phone, location details, and driving habits and time in order to take decisions about insurance.
4. ***Lack of Common Standard:*** Since there are many standards for IoT devices and IoT manufacturing industries, it is a big challenge to distinguish between permitted and non-permitted devices connected to the internet.

5. ***Technical Concerns:*** Due to the increased usage of IoT devices, the traffic generated by these devices is also increasing. Hence, there is a need to increase network capacity and also to store the huge amount of data for analysis and further final storage.

6. ***Security Attacks and System Vulnerabilities:*** There has been a lot of work done in the scenario of IoT security till now. The related work can be divided into system security, application security, and network security

    a. System Security: System security mainly focuses on overall IoT system to identify different security challenges, to design different security frameworks and to provide proper security guidelines in order to maintain the security of a network.
    b. Application security: Application Security works for IoT application to handle security issues according to scenario requirements.
    c. Network security: Network security deals with securing the IoT communication network for communication of different IoT devices.

Protecting Your IoT Devices

Everyone wants to leverage the power IoT devices securely and effectively. These devices have wonderful features to make our life easier, can help to save money and increase the physical security of your home. As the technology grows and security issues build up, most of us will be left with no choice but to purchase or use IoT devices. Here are some steps you can take to protect your IoT devices and yourself.

- Connect Only What You Need:The simplest way to secure an IoT device is to not connect all devices to the Internet. If you do not need your device to be online, don't connect it to your Wi-Fi network.

- Separate Wi-Fi network: It is better to create separatewi-fi network for the devices that need to be connected to IoT. Many Wi-Fi access points have the ability to create additional networks,

named as a Guest network. Another option is to purchase an additional Wi-Fi access point just for IoT devices. This keeps your IoT devices on an isolated network, where cyber criminals cannot be used to harm or attack.

- Update When Possible:Just like your Personal Computer and mobile devices, keep your IoT devices up- to-date. If your IoT device has the option to automatically update, enable that.

- Strong Passwords: Change any passwords on your IoT device to a unique, strong password. Consider using a password manager to securely store all of them.

- Privacy Options:If your IoT device allows configuring privacy options, it is better to disable the amount of information it shares.

IoT devices were not developed with cyber security in mind. But as awareness for cyber security grows, more and more IoT devices come equipped with security features in their devices.

Case Studies

CASE 1: THE MIRAI BOTNET

In October of 2016,the largest DDoS attack happened on service provider 'Dyn'using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN. This IoT botnet was made possible by malware called 'Mirai'. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to login, infecting them with malware. These devices were things like digital cameras and DVR players.

CASE 2: THE HACKABLE CARDIAC DEVICES

It was found that implantable cardiac devices of a particular brand have reported vulnerabilities that could allow a hacker to access the device. Once in, they could drain the battery or administer incorrect pacing or shocks. The devices, like pacemakers and defibrillators, are used to monitor and control patients heart functions and prevent heart attacks. The vulnerability occurred in the transmitter that reads the device's data and remotely shares it with physicians. Hackers could control a device by accessing its transmitter.

CASE 3: THE WI-FI BABY HEART MONITOR REPORTED VULNERABILITIES

The wi-fi Baby Heart monitor was built with good intentions to help parents to monitor their new born babies. This case is an example of how devices with the best of intentions, such as alerting parents when their babies experience heart troubles, can turn dangerous if taken advantage of by a criminal. This threat has to be solved at the hardware layer of the device. In case of embedded computing within the device, the connectivity element aids for exploitation. The manufacturers and developers have to consider this issue and take extra steps to secure the devices at the hardware layer.

CASE 4: CAR BEING HACKED

In this case the main threat was the firmware update vulnerability, where the attackers hijacked the vehicle over the cellular network and they were able to increase or decrease the speed and even deviate from the road. This has proved as a major threat to the concept of emerging Internet of Things (IoT). While companies often ignore the security of peripheral devices or networks, this proved that consequences can be disastrous.

CASE 5: WEBCAM HACKED

Webcams are generally used for home/office security, baby monitoring, etc... and the manufacturing companies claim they are secure. However, a fault in the software can let anyone who obtained a camera's IP address look through it and sometimes listen as well. It was reported in January 2012 that a well-known brand of webcam has transmitted user login credentials in clear, readable text over the Internet. It is basic security practice to secure IP addresses against hacking and to encrypt login credentials or at least password-protect them.

Security lessons that we learn from the above incident:

- Changing the default username and password should be mandatory for the installation of any device on the Internet.
- Passwords for IoT devices should be unique per device, especially when these are connected to the Internet.
- Always patch IoT devices with the latest software and firmware updates to mitigate vulnerabilities.

References

- *https://www.sans.org/security-awareness-training/ouch-newsletter/2016/internet-things-iot*
- *https://thesai.org/Downloads/Volume8No6/Paper_50- Security_Issues_in_the_Internet_of_Things.pdf*
- *https://blog.cyberint.com/what-lures-cyber-criminals-towards-the-internet-of-things*
- *https://royalsociety.org/~/media/events/2017/10/tof-iot/iot-conference%20report-final.pdf*
- *https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_414.pdf*
- *https://resources.infosecinstitute.com/cyber-threat-analysis-aviation-industry/#gref*

Tips for Data Protection

- Backup your data.
- Use "passphrases" rather than "passwords."
- Overwrite deleted files.
- Use a firewall.
- Be cautious of free Wi-Fi networks.

InfoSec CONTEST

InfoSec QUIZ

1. IoT components cannot support _____ security schemes due to low power and less resource with respect to computing capabilities
   a). Complex
   b). Simple
   c). Privacy

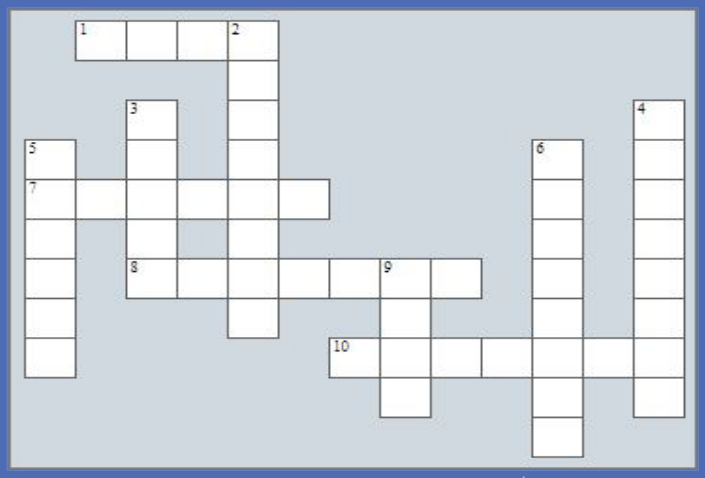
2. If an attack is carried on a network and it alters the integrity of data or modifies the data. This is called an _____attack.
   a). Low Level
   b). Medium Level
   c). High Level

3. _____attacks mainly accounts for unauthorized discovery and mapping of systems, services, or vulnerabilities.
   a). Reconnaissance
   b). Physical
   c). Access

4. _____enables attackers to discover information that cannot be obtained from databases.
   a). Data mining
   b). Malware
   c). DOS Attacks

5. SSL vulnerability wasrecently found on a line of a_____, in a penetration test that was part of an IoT hacking challenge.
   a). Smart camera
   b). Smart Fridges
   c). Smart TV

6. Smart TVs have a challenge of securing _____of the user during transmission.
   a). Network security
   b). Wi-fi security
   c). Data privacy



InfoSec CROSSWORD

Across

1. RASP, protects one of the most critical parts of a device its _____ whether or not it knows the designation of a cyber threat.
7. Smart _____ is the heart of Home –IoT App
8. security deals with securing the IoT communication network for communication of different IoT devices.
10. In a _____attack, an intruder just senses the node or may steal the information but he never attacks physically.

Down

2. The _____concern is the biggest challenge in IoT.
3. Most IoT devices are operated without _____presence.
4. The Internet of Things, also termed as IoT, is nothing but everyday devices connected to _____
5. The _____attacks disturb the performance of IOT physically.
6. _____a user's movement can be tracked by the devices unique identification number.
9. The IoT has a major role in integrating the virtual world and the _____world on the same platform.

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

INFORMATION SECURITY AWARENESS WORKSHOP

JNRM College@Portblair

Awareness Program for Teachers @ Mumbai

ISEA awareness@WestBengal

Jain vidya prasark BEd college@Pune

ISEA Awareness @SVP National Police Academy, Hyderabad

Cybercrime awareness week 2019 inauguration @Andaman & Nicobar Islands

Try Command@Portblair, Andaman & Nicobar Islands

Kendriya vidyalaya AFS@ Begumpet,Hyderabad

IoT Controller

IoT Controller, an Internet of Things (IoT) based app which entertains MQTT Protocol to Monitor and Control your Devices. This application is fully dynamic and flexibly suits any of the IoT devices. By using this App you can Control (ON/OFF) your Devices by giving any Name and Data Topic of your choice. Monitor your device data by customizing the device name, datatopic, prepend & append values. This also provides an Interactive User Interface.

https://play.google.com/store/apps/details?id=com.mywork.androidology.iotcontroller&hl=en

Home-IoT

Home-IOT is the next generation IoT. Home Automation and Personal Security solution designed by WiFly-City in Taiwan. The IPC-9850MA Smart Camera is the heart of this solution, with unique integration of personal security system, temperature and humidity control, remote surveillance system, and home electronic control into 1 single device.This integration dramatically eliminated the system complexity, and the necessity of other additional hardware accessories for the IoT system, as well as reducing labor cost for the installations. Home-IOT System is highly integrated, and very advanced, but super user friendly at the same time. It is designed for users in all ages to experience the new IoT era, which includes a more comfortable, a more convenient and more environmental life style!

https://play.google.com/store/apps/details?id=net.ezhome.smarthome

Onebee Smart IoT

Switch On your Smart Things, Now you Can control your Home/ Office Lights,Fan ,AC, Water Heater , Automatic Gate and Many Home Appliances With Onebee's Smart Server ,
Also Live Viewing and Recorded Videos Of Your CCTV IP camera. Activate / Deactivate Your Home Alarm System and Monitor Your Home Security 24/7 With Mobile app and Notifications.

https://play.google.com/store/apps/details?id=com.smart.meian.onebee

InfoSec

TOOLS

By using rogue connected devices an attacker can collect personal data from a smart camera used at your home for security. So to provide full protection for you IoT devices the following commercial tools can be relied on while enjoying the benefits of the IoT.

Promon SHIELD™

Promon SHIELD™ can protect smart and IoT devicesin ways that conventional antivirus solutions cannot. Traditional security approaches are only as useful as antivirus makers are aware of threats that the cybersecurity industry has published. Runtime Application Self-Protection is a security technology that is built or linked into an application or application runtime environment. When the RASP software sees that malware is changing the permissions attached to an application, RASP will modify the activity of the application to ensure the attack is not satisfactory. RASP, however, protects one of the most critical parts of a device – its apps – whether or not it knows the designation of a cyber threat.

https://promon.co/security-news/protect-iot-devices-apps/

Cloakware

It is security software that protects IoT platforms, APIs and apps. In sensitive industries like industrial IoT, healthcare, finance, and defense, more robust security is needed inside the software itself.
Irdeto's Cloakware is a comprehensive software protection solution that consists of a set of anti-hacking technologies that add extra layers of security to software platforms, apps and endpoint devices. It prevents hackers from reverse engineering by using anti-debug, code and data transformations, whitebox cryptography and other technologies. The secure code is generated with a changeable seed that can be renewed easily to frustrate any long-term hacking attempt. This makes the original code and data virtually impossible to tamper with.

https://irdeto.com/iot-security/

AWS IoT Device Defender

AWS IoT Device Defender is a fully managed service that helps you secure your fleet of IoT devices. AWS IoT Device Defender continuously audits your IoT configurations to make sure that they aren't deviating from security best practices. It also lets you continuously monitor security metrics from devices and AWS IoT Core for deviations from what you have defined as appropriate behavior for each device. If something doesn't look right, AWS IoT Device Defender sends out an alert so you can take action to remediate the issue.

https://play.google.com/store/apps/details?id=com.smart.meian.onebee

SERVHELPER MALWARE

There are public reports about spreading of malware named as ServHelper malware. It is a backdoor malware used by the attacker to steal the information from victim machine to use it in a later stage for performing malicious activity. The mode of spreading of this malware is through the mail which carries either the malicious macro embedded document in the form of Doc, wiz, and pub or through malicious URLs which link to the malware.

- Once the victim enables the embedded macro, it downloads and executes the ServHelper malware on the victim machine.
- After the victim is infected with ServHelper, attacker exploits the victim machine through two ways. First is "tunnel" variant in which attacker access the victim machine through Remote Desktop Protocol via SSH tunnels. After building the connection to Command and control server (C2) controlled by attacker, the attacker performs different malicious activity via executing commands like copying victim browser profiles data, credentials, kill process, create scheduled task and delete malware from the victim machine.
- The Second one is by deploying another Remote Access Trojan (RAT) on victim machine named as FlawedGrace. This RAT creates the configuration file at location C:\ProgramData\.dat which contains the details of C2 IP and Ports to which machine needs to connect. After building connection with C2, malware performs activity via executing different commands like update, remove, download, destroy etc. The IOC of attack is listed below for your action.

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

CERT-In Vulnerability Note CIVN-2019-0034

Denial of Service Vulnerability in Microsoft IIS

Software Affected

- Windows 10 Version 1607 for 32-bit Systems and x64-based Systems
- Windows 10 Version 1703 for 32-bit Systems and x64-based Systems
- Windows 10 Version 1709 for 32-bit Systems and x64-based Systems
- Windows 10 Version 1709 for ARM64-based Systems
- Windows 10 Version 1803 for 32-bit Systems and x64-based Systems
- Windows 10 Version 1803 for ARM64-based Systems
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server, version 1709 (Server Core Installation)
- Windows Server, version 1803 (Server Core Installation)

Overview

A vulnerability has been reported in Microsoft Internet Information Services (IIS), which could be exploited by a remote attacker to cause denial of service (DoS) condition on the target system.

Description

This vulnerability exists in Microsoft Internet Information Services (IIS), which could be exploited by a remote attacker by sending HTTP/2 request with too many SETTINGS frames until one terminates such malicious connection.

Successful exploitation of this vulnerability could cause a severe spike in CPU utilization on an IIS server resulting in denial of service (DoS) conditions.

Solution

Install the February non-security update ADV190005 After applying the updates, administrators need to configure the HTTP/2 limitation of threshold

References

Microsoft
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190005
https://support.microsoft.com/en-us/help/4491420/define-thresholds-on-the-number-of-http-2-settings-parameters-exchange

For more details visit:

https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2019-0034

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)