InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Voice Controllable System Open to laser based audio injection
2. Vulnerabilities in Amazon's Ring Video Doorbell
3. Amazon Kindle , Embedded Devices Open to Code-Execution
4. First Bluekeep Attacks
5. Facebook Reveals new data Leak Incident Affecting Groups Member
6. India's doomed moon mission was hacked by North Korea

10/11/2019

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE ' s that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, ebay, eset, bugcrowd, under armour, coinbase, CCM, etc have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team ' s professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

1. **Voice Controllable System open to laser based audio injection**

Description	
MEMS microphones have light commands vulnerability which allows attackers to remotely inject inaudible and invisible commands into voice assistants, such as Google Assistant, Amazon Alexa, Facebook Portal, and Apple Siri sing light. Academics researchers from the University of Electro-Communications (Tokyo), University of Michigan demonstrated this effect. In addition to sound, microphones also react to light aimed directly at them. Thus, by modulating an electrical signal in the intensity of a light beam, attackers can trick microphones into producing electrical signals as if they are receiving genuine audio. A key issue that could force OEMs to adapt threat models is that most voice-command systems lack proper user authentication because it's assumed that users must be close to the device, which is typically shielded by walls, doors and windows. Light-based command injection may change the equation.	
Source	https://lightcommands.com/20191104-Light-Commands.pdf
Infected Technology	Voice Assistants

2. **Vulnerabilities in Amazon's Ring Video Door Bell**

Description	
A high-security vulnerability in Amazon's Ring Doorbell Pro devices has been discovered which could allow attackers to steal WiFi passwords and launch a variety of cyber attacks against other devices connected to the network. When we enter the configuration mode to setup the device a built in unprotected wireless access point is turned on, allowing the RING app to automatically connect to the doorbell. The researchers discovered that besides using an access point with no password, the initial communication between the RING app and the doorbell is performed insecurely through plain HTTP which may allow an attacker to connect to the same wireless access point during the setup process and steal the WiFi password using a man-in-the-middle attack.	
Source	https://labs.bitdefender.com/2019/11/ring-video-doorbell-pro-under-the-scope/
Infected Technology	Amazon's Ring Video Door bell
Recommendation	Update the latest patch available

3. Amazon Kindle, Embedded Devices Open to Code-Execution

Description
Multiple vulnerabilities have been found in Das U-Boot, a universal bootloader commonly used in embedded devices like Amazon Kindles, ARM Chromebooks and networking hardware which includes both local and remote paths to exploitation. They include a recursive stack overflow, buffer-overflows and double-free memory corruption flaws which allows open door to denial -of -service attacks, device takeover and code-execution. These flaws could allow attackers to gain full control of an impacted device's CPU and modify any thing they choose.

Source	https://threatpost.com/amazon-kindle-embedded-devices-code-execution/150003/
Infected Technology	Amazon Kindle
Recommendation	Update the patch when available
CVE_ID	CVE-2019-13103, CVE-2019-13104, CVE-2019-13105, CVE-2019-13106

4. First Bluekeep Attacks

Description
Microsoft disclosed a serious hackable flaw known as BlueKeep earlier this year and such an attack of mass hacking has finally occurred. The Blueekeep hacking installs a cryptocurrency miner, leeching a victim's processing power to generate cryptocurrency. It is not an automated worm to spread malware like the one predicted, which the BlueKeep vulnerability is capable of. The attackers have scanned the Internet for vulnerable machines to exploit rather than a worm that jumps assisted from one computer to another.

Source	https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/
Infected Technology	Windows
Recommendation	Update the patch released

5. Facebook reveals new data Leak Incident Affecting Groups' Member

Description	
Facebook revealed a new security incident that affected the FB groups member by nearly 100+ 3rd party apps that accessed the group member's information.These apps were misused the Facebook Groups API and retained access to group member information, such as names and profile pictures with group activities.	
Source	https://thehackernews.com/2019/11/facebook-groups-data-leak.html
Infected Industry	Social media

6. India's Doomed moon mission was hacked by North Korea

Description	
INDIA's Space Research Organisation was possibly targeted by North Korean hackers as it tried to land a space craft on the moon for the first time in the country's history.It's feared bungling space station employees may have opened standard phishing emails - the kind of spam you get in your inbox on a weekly basis - and released malware into the top-secret space station's system.	
Source	https://www.dailymail.co.uk/news/article-7663917/Indias-doomed-moon-mission-hacked-North-Korea-cyber-experts-believe.html
Infected Industry	Space research organization

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**