InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Android Ransomware Infect You through SMS Message
2. Apple iOS flaw could allow attacker access via iMessage
3. Capital One data breach
4. New vulnerabilities on WPA3
5. New Mirai botnet hides C2 server in the tor network
6. Cisco paid $8.6m for selling vulnerable VSM to US Government

04/08/2019

www.cryptogennepal.com

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. Android Ransomware Infect You through SMS Message

Description

A new malware dubbed Android/Filecoder.C is being spread through malicious posts. Most malicious posts and comments lure victims into downloading the malware by associating with inappropriate material through bit.ly links.

Once installed on an android phone, Filecoder plunders the victim's contact list and send message to every entrant. The link is advertised as an app which has apparently used the contact's photos, whereas, it is a malicious app harboring the ransomware.

Source	**https://www.darkreading.com/mobile/47–of-android-anti-malware-apps-are-flawed/d/d-id/1335422**
Severity	**Critical**
Infected Technology	**Android**
Recommendation	**Do not download and install apps from unknown sources**

2. Apple iOS flaw could allow attacker access via iMessage

Description	
An iMessage vulnerability in apple iOS could allow attackers to gain access to iOS devices and read their contents using a malicious iMessage as an attack vector. An attacker could also exploit the flaw to remotely read one-time-passwords sent via SMS. An iMessage issue is caused by _NSDataFileBackedFuture class that can deserialize the buffer and it allows an NSData object to be created with length that is different than the length of its bite array. This can allow out of bound reads and out of bounds writes.	
Source	https://www.bleepingcomputer.com/news/security/apple-imessage-flaw-lets-remote-attackers-read-files-on-iphones/
Severity	Critical
Infected Technology	Android
Recommendation	Do not download and install apps from unknown sources

3. Capital One data breach

Description
Capital One-the fifth largest U.S. credit-card issuer and banking institution has recently suffered a data breach exposing the personal information of more than 100 million credit card applicants in the united states and 6 million in Canada. The data breach allowed attackers to steal information of customer that includes approximately 140,000 social security numbers and 80,000 account numbers linked to American customers, and 1 million Canadian social insurance numbers.

Source	https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html
Severity	Critical
Infected Technology	Android
Recommendation	Do not download and install apps from unknown sources

4. New vulnerabilities on WPA3

Description	
Previously, a team of infosec researchers discovered a vulnerability in the new wireless security protocol that could allow attackers to recover the password of the Wi-Fi network dubbed 'DragonBlood'. The same group of researchers have again discovered two new vulnerabilities on WPA3. The two newly reported vulnerabilities are named CVE-2019-13377 and CVE-2019-13456.	
Source	https://www.technadu.com/two-dragonblood-vulnerabilities-wpa3-wi-fi-standard/75933/
Infected Technology	Wi-Fi WPA 3

5. New Mirai botnet hides C2 server in the tor network

Description	
Researchers from Trend Micro have discovered Mirai botnets using C2 in the Tor to maintain anonymity and make takedowns much harder. Mirai first appeared in 2016 when researchers discovered its attack on the IoT devices. The new variant of Mirai was spotted using TCP ports 9527 and 34567.	
Source	https://securityaffairs.co/wordpress/89237/malware/mirai-botnet-tor-c2.html
Severity	Critical
Recommendation	Change all default credentials and common passwords to some stronger passwords

6. Cisco paid $8.6m for selling vulnerable VSM to US Government

Description

A vulnerability on Cisco’s video surveillance manager could lead hackers to gain unauthorized access to the data stored in the surveillance manager, turn off cameras and even gain administrative access on the client’s network. A security researcher has claimed he reported the issue back in 2011 but cisco failed to patch the vulnerability. Cisco paid $8.6m to the US federal government and 16 states for products purchased between 2008 and 2013.

Source	https://www.zdnet.com/article/cisco-to-pay-8-6-million-for-selling-vulnerable-software-to-us-government
Recommendation	The issue has been patched in a software update.

For any queries/recommendations:

Contact us: whois@cryptogennepal.com