InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. 3 Google Play Store Apps Exploit Android Zero-Day
2. Paypal Password Exposed
3. TikTok faced multiple vulnerabilities
4. Cable Modems are vulnerable to Cable Hunt Vulnerability
5. Zero Day Vulnerability in Firefox

13/01/2019

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. **3 Google Play Store Apps Exploit Zero-day**

Description	
A malicious application in the Google Play store targeted a recently patched zero-day vulnerability that affects multiple Android devices, including Google's Pixel phones.Tracked as CVE-2019-2215, the vulnerability was disclosed as a zero-day in October by Google Project Zero security researcher Maddie Stone. A use-after-free in the binder driver, the bug could lead to an exploitable crash.The flaw was initially addressed in December 2017 in the 4.14 Linux kernel, the Android Open Source Project (AOSP) 3.18 kernel, AOSP 4.4 kernel, and AOSP 4.9 kernel. Two years later, it was still impacting Pixel 2; Pixel 1; Huawei P20; Xiaomi Redmi 5A, Redmi Note 5, and A1; Oppo A3; Motorola Moto Z3; LG phones running Android 8 Oreo; and Samsung Galaxy S7, S8 and S9 models.	
Source	https://thehackernews.com/2020/01/android-zero-day-malware-apps.html
Infected Technology	Smart Phones
Recommendation	Keep devices and apps up-to-date Always pay close attention to the permissions requested by apps
CVE_ID	CVE-2019-2215

2. Paypal Password Exposed

Description	
A software wiz discovered a "high-severity" bug that put users' data at risk, but the company fixed it before anyone's personal information could be "exposed."The vulnerability, which could have allowed hackers to snag PayPal users' passwords, was disclosed this week.	
Source	https://medium.com/@alex.birsan/the-bug-that-exposed-your-paypal-password-539fc2896da9
Infected Industry	Paypal
Recommendation	Never Store Password In Plain text Update the patch when available

3. Tiktok faced Multiple vulnerabilities

Description	
Multiple vulnerabilities were discovered within a popular app named TikTok, these vulnerabilities allow attackers to get a hold of TikTok accounts and manipulate their content, delete videos, upload unauthorized videos, make private "hidden" videos public and also reveal personal information saved on the account such as private email addresses. TikTok has a functionality that lets users send an SMS message to themselves in order to download the application, but attackers can capture the HTTP request that contains mobile numbers and can send SMS messages which contains malicious link to any phone number on behalf of TikTok.	
Source	https://research.checkpoint.com/2020/tik-or-tok-is-tiktok-secure-enough/
Infected Technology	TikTok
Recommendation	Update the patch when available

4. Cable Modems are vulnerable to Cable Hunt Vulnerability

Description	
Cable Haunt is a critical vulnerability found in hundreds of cable modems from various manufacturers across the world. The vulnerability enables remote attackers to execute arbitrary code on your modem, indirectly through an endpoint on the modem. Your cable modem is in charge of the internet traffic for all devices on the network. Cable Haunt might therefore be exploited to intercept private messages, redirect traffic, or participation in botnets.An attacker can also conduct buffer overflow to exploit and gain control of the modem. Using Cable Hunt an attacker could change default DNS server, COnduct remote Man-in-the-middle attacks, Disable ISP firmware upgrade, change every config file and settings, get and set SNMP OID values, change all associated MAC address and change serial numbers.	
Source	https://www.zdnet.com/article/hundreds-of-millions-of-cable-modems-are-vulnerable-to-new-cable-haunt-vulnerability/
Infected Technology	Cable Modems
Recommendation	Update its firmware Change its default password

5. **Zero Day Vulnerability In FireFox**

Description	
A 'type confusion vulnerability' has been discovered in firefox. It resides in the IonMonkey just-in-tie(JIT) compiler of the Mozilla's JavaScript engine SpiderMonkey. A type vulnerability occurs when the code doesn't verify what objects it passed to and blindly uses it without checking its type, allowing attackers to crash the application or achieve code execution. An attacker can trick an unsuspecting user into visiting a maliciously crafted webpage to execute arbitrary code on the system within the context of the application via this exploit. Mozilla has patched this vulnerability in Firefox 72.0.1 and Firefox ESR 68.4.1 versions. Users have been advised to ensure that their firefox browsers are updated to the latest versions. To manually update firefox navigate to Home > Help > About Firefox .	
Source	https://www.mozilla.org/en-US/security/advisories/mfsa2020-03/
Infected Technology	FireFox
Recommendation	Update the patch when available

For any queries/recommendations:

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