August 10, 2020

INFOSEC WEEKELY

#MADE4SECURITY

- 20 GB of source code and internal documents of Intel leaked from breach
- 50% of Smartphones affected by Snapdragon bugs
- KrØØk attack variants impact Qualcomm, MediaTek Wi-Fi chips
- Apple Touch ID Flaw Could Have Let Attacker Hijack iCloud Account
- Http Request Smuggling Attacks
- US Government Warns of a New Strain of Chinese 'Taidoor' Virus
- Unpatched Bug in Windows Print Spooler Lets malware run as admin

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. 20 GB of source code and internal documents of Intel leaked from breach

Description	
Classified and confidential documents of Intel have been uploaded to public facing file server. The shared file has been accessed from a breach and has been released as first part of the leaks. The leak dubbed as "Juicy" has been released anonymously and contains various tools, source code for various platform, confidential information related to unreleased platform, training videos and various other internal classified information. The leaked data is part of the breach that happened earlier this year.	
Source	https://www.bleepingcomputer.com/news/security/intel-leak-20gb-of-source-code-internal-docs-from-alleged-breach/
Infected Technology	Intel

2. 50% of Smartphones affected by Snapdragon bugs

Description	
Various vulnerabilities in Qualcomm's Snapdragon chip Digital Signal Processor (DSP) could allow attackers to take control of more than 40% of the smartphone without user interaction which allows to spy on the phone and install un-removable malware. The vulnerable chip in available in almost every Android device including flagship devices. The vulnerability has been identified by researcher at Checkpoint, Qualcomm has fixed the vulnerabilities and made it available to mobile vendors.	
Source	https://blog.checkpoint.com/2020/08/06/achilles-small-chip-big-peril/
Infected Technology	Qualcomm's Snapdragon
CVEs	CVE-2020-11201, CVE-2020-11202, CVE-2020-11206, CVE-2020-11207, CVE-2020-11208 and CVE-2020-11209
Recommendation	• Apply the security update once released by mobile vendors

3. KrØØk attack variants impact Qualcomm, MediaTek Wi-Fi chips

Description	
KrØØk, an information disclosure vulnerability disclosed by ESET, has impacted Qualcomm and MediaTek Wi-Fi chips. This vulnerability can be used to decrypt WPA-2 encrypted wireless network packets by forcing them to use all-zero encryption keys to encrypt the traffic. The vulnerable chips are most popular among smartphone, Laptops, smart watch, Assistant devices and various network devices including routers. The vulnerability has been patched by various vendors including Amazon (Echo, Kindle), Apple, Google, Samsung, Raspberry Pi, Xiaomi as well as some access points by Asus and Huawei.	
Source	https://www.welivesecurity.com/2020/02/26/krook-serious-vulnerability-affected-encryption-billion-wifi-devices/
Infected Technology	Wi-Fi Chips by: • Qualcomm • MediaTek • Broadcom • Cypress
CVEs	CVE-2019-15126
Recommendation	• Update the patch released by your device manufacturer

4. Apple Touch ID Flaw Could Have Let Attacker Hijack iCloud Account

Description	
A security flaw in iOS and macOS that could have potentially allowed an attacker to gain unauthorized access to user's iCloud account. The flaw resided in Apple's implementation of Touch ID (or Face ID) biometric feature that authenticated users to log in to websites on Safari, especially those that use Apple ID logins. When users try to sign in to a website that requires an Apple ID , a prompt is displayed to authenticate the login using Touch ID- which skips the two-factor authentication step since it already leverages a combination of factors for identification, such as the device and biometric information.	
Source	https://thehackernews.com/2020/08/apple-touchid-sign-in.html
Infected Technology	iOS, macOS
Recommendation	Update the latest patch available from Apple

5. Http Request Smuggling Attacks

Description	
The Four New variants of HTTP request smuggling attacks were disclosed at Black Hat USA. The attack vector is a class of web security vulnerability that can lead to variety of problems, including cache poisoning, session hijacking, and the circumvention of security filters. First web security researcher demonstrated how isolated HTTP requests can be manipulated to desynchronize message processing and explored how reverse proxies can be abused to mount an HTTP header smuggling attack. This attack technique can be utilized to bypass authentication checks, steal data, compromise back-end systems, hijack user request, poison web cache and many more.	
Source	https://thehackernews.com/2020/08/http-request-smuggling.html
Infected Technology	Aprelium's Abyss, Microsoft IIS, Tomcat, Nginx, Squid, HA Proxy, Caddy, Traefik, varnish,
Recommendation	Update their product and secure against HTTP Request Smuggling

6. US Government Warns of a New Strain of Chinese 'Taidoor' Virus

Description	
Three agencies of US government have published a joint alert alerting US private entity about new versions of Taidoor, a malware family previously associated with Chinese state-sponsored hackers. The three agencies say this malware has been used since 2008 and wildly spotted in 2012 and 2013.The new Taidoor samples have versions for 32- and 64-bit systems and are usually installed on victim's systems as a service DLL. This DLL file contains two other files. The first one is a loader, which is started as a service. The loader decrypts the second file, and executes it in memory, which is main Remote Access Trojan (RAT).	
Source	https://thehackernews.com/2020/08/chinese-hacking-malware.html
Recommendation	• Users and Administrators keep their OS patches up to date • Disable File and Printer Sharing services • Enforce Strong Password Policy • Be cautious when opening email attachment

7. Unpatched Bug in Windows Print Spooler Lets malware run as admin

Description	
Windows users have been warned to ensure their security protections are up to date following the disclosure of a new bug that could affects printer services. Researchers were able to bypass recent patches to exploit flaw that could allow hackers to take over a private network after hijacking individual printing devices. The flaw affects windows Print Spooler, the service that manages the printing process, giving third parties that could be exploited to run malware.	
Source	https://www.bleepingcomputer.com/news/security/unpatched-bug-in-windows-print-spooler-lets-malware-run-as-admin/
Infected Technology	Microsoft Print Spooler
CVE_ID	CVE-2020-1048 CVE-2020-1337
Recommendation	Update the next patch available

For any queries/recommendations:

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