InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Android Camera App bug lets apps record video without permission
2. D-Link routers vulnerable to Remote Code Execution (RCE) Vulnerability and stated they won't fix
3. New 'Critical Microsoft Windows Update' spam attempt discovered
4. Millions of Sites Exposed by Flaw in Jetpack WordPress Plugin
5. Flaws found in 4 different VNC Software
6. Flaws found in Qualcomm Chips
7. WhatsApp patch critical vulnerability capable of installing spyware
8. Intel CPU impacted by new ZombieLoad side-channel attack
9. WannaMine found exploiting in the wild

25/11/2019

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, Trip Advisor, 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 Camera App bug lets apps record video without permission

Description
A new vulnerability has been found in the camera apps for millions on android that could allow other apps to record video, take pictures and extract GPS data from media without having the required permission. The vulnerability is known to affect the Google camera and Samsung Camera.

Source	https://www.bleepingcomputer.com/news/security/android-camera-app-bug-lets-apps-record-video-without-permission/
Infected Technology	Android camera
CVE	CVE-2019-2234
Recommendation	Update your camera app and android version when available

2. D-Link routers vulnerable to Remote Code Execution (RCE) Vulnerability and stated they won't fix

Description
D-Link has warned that more of its routers are vulnerable to critical flaws that allow remote hackers to take control of hardware and steal data. The routers won't be fixed, said D-Link, explaining that the hardware has reached its end-of-life and will no longer receive security updates.

Source	https://www.cybersecurity-review.com/news-august-2019/russian-hacking-group-targeting-banks-worldwide-with-evolving-tactics/
Infected Models	DIR-866, DIR-655, DHP-1565, DIR-652, DAP-1533, DGL-5500, DIR-130, DIR-330, DIR-878, DIR-615, DIR-825, DIR-835, DIR-855L and DIR-862
Recommendations	Change the affected models

3. New 'Critical Microsoft Windows Update' spam attempt discovered

Description	
A new spam campaign pretending to be a 'Critical Microsoft Windows Update' has been discovered that attempts to deliver the Cyborg Ransomware. Researchers outline how an attacker is sending spam email that pretends to be a 'Critical' Windows update and prompts the recipient to install it. The supposed Windows update attached to the email is a downloader for the Cyborg Ransomware executable that has been renamed to a random named jpg image file.	
Source	https://www.bleepingcomputer.com/news/security/critical-windows-update-spam-fails-at-delivering-ransomware/
Infection Method	Email Spam
Recommendation	Do not open attachments in suspicious emails

4. Millions of Sites Exposed by Flaw in Jetpack WordPress Plugin

Description	
Jetpack is an extremely popular WordPress plugin that provides free security, performance, and site management features including site backups, secure logins, malware scanning, and brute-force attack protection. Not much has been released by the developers, but they urge to update to the latest version of the plugin.	
Source	https://www.bleepingcomputer.com/news/security/millions-of-sites-exposed-by-flaw-in-jetpack-wordpress-plugin/
Infected Technology	Wordpress Plugin
Recommendation	Update to the latest version of Jetpack Wordpress Plugin

5. Flaws found in 4 different VNC Software

Description	
Four popular open-source VNC remote desktop applications have been found vulnerable to a total of 37 security vulnerabilities, many of which went unnoticed for the last 20 years and most severe could allow remote attackers to compromise a targeted system. The four applications include: 1) LibVNC, 2) UltraVNC 3) TightVNC 4) TurboVNC. Some of the discovered security vulnerabilities can also lead to remote code execution (RCE) attacks, meaning an attacker could exploit these flaws to run arbitrary code on the targeted system and gain control over it.	
Source	https://thehackernews.com/2019/11/vnc-remote-software-hacking.html
Infected Technology	VNC Software
Recommendation	Keep your application updated; TightVNC is no longer supported

6. Flaws found in Qualcomm Chips

Description	
Millions of Android phones and tablets exposed to a severe vulnerability due to a flaw found in Qualcomm chips. This flaw could allow attackers to steal sensitive data stored in a secure area that is otherwise supposed to be the most protected part of a mobile device. The vulnerabilities reside in Qualcomm's Secure Execution Environment (QSEE), an implementation of Trusted Execution Environment (TEE) based on ARM TrustZone technology. Along with other personal information, QSEE usually contains private encryption keys, passwords, credit, and debit card credentials.	
Source	https://research.checkpoint.com/the-road-to-qualcomm-trustzone-apps-fuzzing/
Infected Technology	Qualcomm Chipset

7. WhatsApp patch critical vulnerability capable of installing spyware

Description	
Whatsapp has recently patched a critical vulnerability which could have allowed attackers to remotely steal chat messages and files stored on the devices. The vulnerability was caused because of the way WhatsApp parse the elementary stream metadata of an MP4 file, which could lead to denial-of-service or remote execution attacks. An attacker can send a maliciously crafted MP4 to the target over WhatsApp which eventually can be used to install a malicious backdoor or spyware on compromised devices silently.	
Source	https://thehackernews.com/2019/11/whatsapp-hacking-vulnerability.html
Infected Technology	WhatsApp
Recommendation	Update your WhatsApp application to the latest version

8. Intel CPU impacted by new ZombieLoad side-channel attack

Description	
A data-leaking side-channel vulnerability also affects the most recent Intel CPUs, including the latest Cascade Lake. ZombieLoad is one of the microarchitectural data sampling speculative execution vulnerabilities that affect intel processor generation released from 2011 onwards. It is a Meltdown-type attack that targets the fill-buffer logic allowing attackers to steal sensitive data not only from other applications and the operating system but also from virtual machines running in the cloud.	
Source	https://www.zdnet.com/article/windows-linux-get-options-to-disable-intel-tsx-to-prevent-zombieload-v2-attacks
Infected Technology	Intel Chipset
CVE	CVE-2019-11135
Recommendation	Update your Webmin as soon as possible

9. WannaMine found exploiting in the wild

Description	
WannaMine v4.0 is the latest variant of WannaMine cryptominer. It leverages the EternalBlue exploit to spread and compromise vulnerable hosts. WannaMine penetrates computer systems through an unpatched SMB service and gains code execution with high privileges to then propagate across the network, gaining persistence and arbitrary code execution abilities on as many machines possible.	
Source	https://www.crowdstrike.com/blog/weeding-out-wannamine-v4-0-analyzing-and-remediating-this-mineware-nightmare/
Infected Technology	Microsoft Windows
Recommendation	Keep system up to date and ensure MS17-010 is patched

For any queries/recommendations:

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