InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Growing Risk of File-based attacks
2. Exfiltrating data from encrypted PDF files
3. New Critical Exim Flaw Exposes Email Servers to Remote Attacks-Patch released
4. ‘checkm8’ jailbreak released for iOS devices
5. Comodo Forums Hack Exposes User’s Data
6. New 0-Day Flaw Affecting Most Android Phones Being exploited in the Wild

06/10/2019

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. Growing Risk of File-based Attacks

Description

Usually small to medium businesses (SMBs) lack the kind of security that protects their larger counterparts. Falling victims to file-based malware can cause enormous problems for SMBs. An attack can damage critical data stored in the organization's computers. Such loss can force a company to temporarily halt operations, resulting in financial losses. A file-based attack involve malware that is kept hidden in a seemingly legitimate document. When a user opens the file, the malware is activated. Depending on the payload, the malware could destroy or steal data.

Source	https://thehackernews.com/2019/10/business-cybersecurity-tips.html
Infected Industry	SMB
Recommendation	User awareness security training

2. Exfiltrating data from encrypted PDF files

Description

Exfiltrating data from PDF files dubbed as PDFex has set new techniques that could allow attackers to access the entire content of a password-protected or encrypted PDF file. PDFex attack allows an attacker to remotely exfiltrate content once a legitimate user opens the document, however attacker cannot remove or know the password for an encrypted PDF. In other words, PDFex technique will send the copy of decrypted content to a remote attacker-controlled server on the internet, without having the corresponding password.

Source	https://thenextweb.com/security/2019/10/02/pdf-flaw-lets-hackers-read-password-protected-documents-researchers-say/
Infected Technology	Web PDF viewer
Recommendation	Update patch when available

3. New Critical Exim Flaw Exposes Email Server to Remote Attacks-Patch Released

Description

Exim is a widely used, open source mail transfer agent (MTA) developed for Unix-like operating systems like Linux, Mac OSX or Solaris. The Exim critical security vulnerability has been discovered which could allow a remote attacker to gain root-level access to the system, cause a denial of service (DoS) condition, execute arbitrary code and simply crash or potentially execute malicious code on targeted servers.

Source	https://www.bleepingcomputer.com/news/security/new-exim-vuln
Infected Technology	Linux , Mac OS
Recommendation	Update the Released patch

4. ‘Checkm8’ jailbreak released for iOS devices

Description

A security researcher released a new jailbreak named 'Checkm8' that impacts iOS devices running on A5 to A11 chipsets. These devices span eight generations, from iPhone 4s to iPhone8 and X. It exploits vulnerabilities in Apple's Bootrom to grant phone owners full control over their device. This is an unpatchable exploit because, as to a software bug that can be updated, this vulnerability is in the hardware. Threat actors might use this exploit to root the devices although this jailbreak requires physical access and can only be triggered over USB. This jailbreak is also not permanent and works only until the next reboot.

Source	https://github.com/axi0mX/ipwndfu
Infected Technology	iOS
Recommendation	iOS users should be aware, and an incentive to upgrade to newer handsets with unaffected chips.

5. Comodo forums Hack Exposes User's Data

Description	
Data breaches in cybersecurity company Comodo exposed login account information of over nearly 245,000 users registered with the Comodo Forums websites. A recently disclosed vBulletin 0-day vulnerability was used by the attacker on the websites. Users have been advised to change their passwords as part of good password practices.	
Source	https://thehackernews.com/2019/10/Comodo-vbulletin-hacked.html
Infected Industry	Company's Bulletin/Forums
Recommendation	Patch immediately when available
CVE ID	CVE-2019-16759

6. New 0-Day Flaw Affecting Most Android Phones being Exploited in the Wild

Description	
Google's 0-Day security researchers have found a critical vulnerability in its android OS that would allow hackers to gain access to gain full access to at least 18 smart phones , including its own Pixel smart phones. The company disclosed the exploit just seven days after discovering it adding that the vulnerability has been used in the wild.	
Source	https://www.engadget.com/2019/10/04/google-zero-day-android-pixel-samsung-huawei/
Infected Technology	Android Smart Phones
Recommendation	Apply the available patch provided by google

For any queries/recommendations:

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