InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

- Playing Specially Crafted Videos Can Lead to RCE on Android
- Multiple Zero-Day Vulnerabilities in Comodo anti-virus Software
- Business Email Compromise (BEC)
- ProFTPD: Arbitrary File Upload Flaw
- 23 Million+ Stolen Credit Cards sold on Dark Web
- Data Leaks from Brazilian Banks

28/07/2019

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. Playing Specially Crafted Videos Can Lead to RCE on Android

Description	
It is an RCE (Remote code execution) vulnerability that affects over 1 billion device running Android OS between version 7.0 and 9.0. The android framework if exploited can execute arbitrary code within the context of a privileged process on a target device. To gain full control of the device, an attacker tricks the user into playing a specially crafted video file with android's native video player application received by email or downloaded through untrusted sites.	
Source	https://thehackernews.com/2019/07/android-media-framework-hack.html
Infected Technology	Android
Recommendation	Do not open videos before validating sender; Update your device if available

2. Multiple Zero-Day Vulnerabilities in Comodo anti-virus Software

Description	
Comodo - antivirus software are used to protect PC's and other systems from unknown malware and threats - riddled with some vulnerabilities that would ultimately grant an attacker complete control over the machine. A sandbox escape and a privilege escalation were noticed in a Comodo system. An attacker could even disable antivirus altogether, leaving the devices/systems unprotected and vulnerable.	
Source	https://www.infosecurity-magazine.com/news/five-zerodays-found-in-comodo/
Infected Technology	Comodo Anti-Virus
Recommendation	Update after patches are available

3. Business Email Compromise (BEC)

Description	
BEC and EAC fraud are very serious issue that is growing rapidly, victims are increasing day by day. At first attacker gains access to the targeted email through social engineering (phishing) or by compromising victim's server and once it gains access to email, it can review the victim's email account to gain information about their financial institutions, accounts, contacts etc. Then with those victims' information, attackers can initiate transactions with the victim's financial institutions from victim's compromised or fake email account.	
Source	https://www.csoonline.com/article/3409069/business-email-compromise-the-odds-of-being-a-victim-are-increasing.html
Infected Technology	Business e-mails
Recommendation	Self-awareness regarding Scam and Phishing e-mails; Do not use common passwords; Review the e-mails, validate the source before interacting with the received e-mail.

4. ProFTPD: Arbitrary File Upload Flaw

Description	
The vulnerability consists of mod_copy module of ProFTPD server, that is a component that allows the user to copy files/directories from one place to another on a server without having to transfer the data to the client and back. An incorrect access control issue in the mod_copy module could be exploited by an authenticated user to unauthorizedly copy any file on a specific location of the vulnerable FTP server where the user is otherwise not allowed to write a file. This may also lead to remote code execution. The mod_copy module allows remote attackers to read and write to arbitrary files via the site CPFR and site CPTO commands.	
Source	https://www.ceos3c.com/news/proftpd-powered-ftp-servers-affected-with-arbitrary-file-copy-flaw/
Infected Technology	ProFTPD: File Transfer Protocol Service
Recommendation	Patch will be sent by the vendors

5. 23 Million+ Stolen Credit Cards sold on Dark Web

Description	
Over 57% visa cards, 29% mastercards and 12% American express third has been stolen by attackers. Attackers use number of techniques to steal credit card data. They can copy the swipes via "skimmers" and also can infect the electronic device with malware, so when the victim makes a transaction, all the credit card details are sent to the hackers. Those credit cards details can be sold for as little as $5.	
Source	https://fossbytes.com/23-million-stolen-credit-cards-sold-on-dark-web-in-the-first-half-of-2019/
Infected Industry	Credit Cards

6. Data Leaks from Brazilian Banks

Description	
Security researchers at Data Group have detected a vulnerability at an unprotected server belonging to a Brazilian services provider. It has exposed a massive batch of data such as scanned ID, social security cards, service request forms and various documents from customers of various local banks.	
Source	https://www.zdnet.com/article/brazilian-banking-users-exposed-by-250gb-data-leak/
Infected Industry	Banking Sector
Recommendation	Update all devices (Firewalls, OS, Routers, etc.) that are available at the organization.

For any queries/recommendations:

Contact us: whois@cryptogennepal.com