InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Google Chrome Affected By Magellan 2.0 Flaws
2. Cisco ASA and Firepower appliance seeing increased attacks
3. ToTok Messaging app is a spying tool
4. Critical Citrix Bug Puts 80,000 Corporate LANs at Risk
5. Two information-disclosing bugs found in Twitter Android

30/12/2019

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. Google Chrome Affected By Magellan 2.0 Flaws

Description	
A new set of SQLite vulnerabilities can allow attackers to remotely run malicious code inside Google Chrome, the world's most popular web browser.The vulnerabilities, five, in total, are named "Magellan 2.0," and were disclosed today by the Tencent Blade security team.All apps that use an SQLite database are vulnerable to Magellan 2.0; however, the danger of "remote exploitation" is smaller than the one in Chrome, where a feature called the WebSQL API exposes Chrome users to remote attacks, by default.	
Source	https://threatpost.com/google-chrome-affected-by-magellan-2-0-flaws/151446/
Infected Technology	Google Chrome
Recommendation	Update the security patch available

2. Cisco ASA and Firepower appliance seeing increased attacks

Description	
Cisco is warning that a vulnerability in the software on its enterprise Adaptive Security Appliances (ASAs) and Firepower firewalls is being exploited in the wild, for denial of service attacks that can crash the devices.The vulnerability stems from incorrect handling of Session Initiation Protocol (SIP) traffic by the inspection engine in Cisco's ASA Software Release 9.4 and FTD Software Release 6.0 and later versions.SIP is used to set up voice over internet protocol phone calls.Remote attackers can crash ASA and Firepower devices by sending large amounts of SIP requests.	
Source	https://www.scmagazine.com/home/security-news/vulnerabilities/cisco-asa-and-firepower-appliance-seeing-increased-attacks/
Infected Industry	Cisco ASA and Firepower Firewalls
Recommendation	Update to a non-affecting version
CVE_ID	CVE-2018-0296

3. ToTok Messaging App is a spying tool

Description	
ToTok, an Emirati messaging app is billed as an easy and secure way to chat by video or text message with friends and family. This app has been downloaded to millions of Phones, even in a country that has restricted popular messaging services like whatsapp and Skype. But the service, ToTok is actually a spying tool, as it is used by the government of United Arab Emirates to try to track every conversation, movement, relationship, appointment, sound and image of those who install it on their phones. The governments are pursuing more effective and convenient methods to spy on foreign adversaries, criminal and terrorist networks, journalists and critics.	
Source	https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html?searchResultPosition=1
Infected Technology	ToTok Messaging App
Recommendation	Update the patch when available

4. Critical Citrix Bug Puts 80,000 Corporate LANs at Risk

Description	
Citrix, a digital workspace and enterprise networks vendor, has suffered a critical vulnerability in Citrix Application Delivery Controller (ADC) and Citrix Gateway. These Citrix products are used for application-aware traffic management and secure remote access, and are installed in at least 80.000 companies in 158 countries. This existing vulnerability could allow an unauthenticated attackers to gain remote access to a company's local network and carry out arbitrary code execution. This attack does not require access to any accounts, and therefore can be performed by any external attacker. This vulnerability allows any unauthorized attacker to not only access published applications, but also attack other resources of the company's internal network from the Citrix server.	
Source	https://threatpost.com/critical-citrix-bug-80000-corporate-lans-at-risk/151444/
Infected Technology	Citrix Server
CVE_ID	CVE-2019-19781

5. Two Information -disclosing bugs found in Twitter Android

Description	
Two vulnerabilities have been identified in twitter android app that where one could cause attackers to view nonpublic account information or control accounts and another that reportedly allowed an attacker to look up details on 17 million accounts. The first vulnerability enable an exploitation via a complicated process involving insertion of malicious code into restricted storage area of the twitter app. With successful exploit an attacker could access information such as direct messages, protected tweets and location information. While second vulnerability allow an attacker to reveal information such as 17 million phone numbers to respective accounts, after uploading huge lists of phone numbers through the contacts upload feature.	
Source	https://www.scmagazine.com/home/security-news/vulnerabilities/two-information-disclosing-bugs-found-in-twitter-android/
Infected Technology	Twitter
Recommendation	Update the patch when available

For any queries/recommendations:

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